A new chaotic map development through the composition of the MS Map and the Dyadic Transformation Map

Suryadi MT, Yudi Satria, Venny Melvina, Luqman N Prawadika, Ita M Sholihat

Department of Mathematics, Universitas Indonesia, Depok, 16424, Indonesia

E-mail: yadi.mt@sci.ui.ac.id, ysatria@sci.ui.ac.id, venny.melvina@sci.ui.ac.id, nuradip.luqman@yahoo.com, summerbreeze91.im@gmail.com

Abstract. In this paper, a new chaotic map is proposed, that is obtained from the composition of two chaotic maps, that is, the MS Map and the Dyadic Transformation Map. The composition process starts from the MS Map, followed by the Dyadic Transformation Map. The resulting composition is a new chaotic function. This is shown by the bifurcation diagram analysis result, Lyapunov Exponents, and the NIST randomness test. The bifurcation diagram shows that the best densities occur at $\lambda / g_{2019} \in (0.3, 5)$ and $g_{1870} = 3.8$. The Lyapunov Exponents has nonnegative values for $r / g_{1870} \in [1, 4]$. The NIST randomness test with initial value and parameters $x_0 = 0.6$, $r = 3.8$, and $\lambda = 3.5$ shows that the new chaotic map passes 14 out of 16 NIST tests.

1. Introduction

In this big data era, most data and informations are served digitally in various storage media that allows public access. These data and informations may be crucial, so their security is on demand. Therefore, a protection method is required for these digital assets, such as an encryption method.

Many algorithms are researched for data encryption, and one of them is the chaos based algorithms. Chaotic functions have been commonly used for keystream generation for data encryption [1]. Currently, many chaotic maps have been produced from researches applied in digital data encryption process [2-18]. Moreover, some observations shows that a random number generator (RNG) that utilizes chaotic maps can be resulted from the combination of two or more chaotic functions [19-20]. This is done for resistance improvement against various attacks when the chaos map is applied for digital data encryption.

Referring from the previous results, specifically that uses the MS Map [21, 22] and the Dyadic Transformation [16], in this paper, a new chaotic map which is the result of the composition of the MS Map and the Dyadic Transformation is developed. This composition is also chaotic, so it can serve as an new alternative as a chaotic RNG.

2. Research Method

The MS Map is a modified version of the Logistic Map, having the equation [21, 22]

$$f(x) = \frac{r x}{1 + \lambda (1-x)^2} (mod 1)$$  (1)
with \( x \mod 1 \) defined as
\[
x \mod 1 = x - \lfloor x \rfloor
\] (2)

Recursively, equation (1) can be represented as
\[
x_{n+1} = \frac{r\lambda x_n}{1 + \lambda(1-x_n)^2} \pmod{1}
\] (3)
with initial value \( x_0 \in (0,1) \).

As for the Dyadic Transformation, its equation is defined as [18]
\[
g(x) = \begin{cases} 2x, & 0 \leq x < 0.5 \\ 2x - 1, & 0.5 \leq x < 1 \end{cases}
\] (4)

Here, the new chaotic map is a composition of the form \( f \circ g \) with \( f \) and \( g \) respectively as in equation (1) and (4). Since the Dyadic Transformation is defined on two partitioned domains, so does the new map, that is,

a) For \( 0 \leq x \leq 0.5 \)
\[
(f \circ g)(x) = \frac{r\lambda 2x}{1 + \lambda(1-2x)^2} \pmod{1}
\] (5)

b) For \( 0.5 \leq x \leq 1 \)
\[
(f \circ g)(x) = \frac{r\lambda(2x-1)}{1 + \lambda(2-2x)^2} \pmod{1}
\] (6)

Therefore, the new map can be defined as
\[
(f \circ g)(x) = \begin{cases} \frac{r\lambda 2x}{1 + \lambda(1-2x)^2} \pmod{1}, & 0 \leq x < 0.5 \\ \frac{r\lambda(2x-1)}{1 + \lambda(2-2x)^2} \pmod{1}, & 0.5 \leq x < 1 \end{cases}
\] (7)

and can be written as the recursion
\[
x_{n+1} = \begin{cases} \frac{r\lambda 2x_n}{1 + \lambda(1-x_n)^2} \pmod{1}, & 0 \leq x_n < 0.5 \\ \frac{r\lambda(2x_n-1)}{1 + \lambda(2-x_n)^2} \pmod{1}, & 0.5 \leq x_n < 1 \end{cases}
\] (8)
with initial value \( x_0 \in (0,1) \). We name this newly recursion as the MSDT Map.

### 3. Result and Analysis
This MSDT Map exhibits chaotic behaviour. This is shown by the bifurcation diagram and the Lyapunov Exponent analysis [1,21,22,23]. Furthermore, referring to the sequence of numbers this map generates, the 16 NIST tests of randomness indicates that the sequence is random [24].

Here, the initial value and parameters of the MSDT map used for the test is \( x_0 = 0.6 \), \( r = 3.8 \), and \( \lambda = 3.5 \).

#### 3.1 Bifurcation Diagram
The bifurcation diagram is a diagram that shows asymptotically visited values of a system as a function of the parameters in the system (based on the following Algorithm 1), from which we can detect chaotic behaviors, that is, when the points are sufficiently dense, the system is chaotic [1,23].
**Algorithm 1.** Bifurcation Diagram:

**Input:** $x_0, \lambda$, dan $r$

**Output:** plots of $x_n$ values

1. Input initial values, parameter values, number of iterations ($i$)
2. For $n = 1$ to $i$
3. Calculate $x_n$ based on the MSDT Map function
4. Plot the value of $x_n$
5. Next $n$
6. Stop

![Bifurcation Diagram](image_url)

**Figure 1.** MSDT Map bifurcation diagram with $r = 3.8$ and $x_0 = 0.6$

As shown in Figure 1, the bifurcation diagram is dense for the initial value $x_0 = 0.6$ and the parameter values $r = 3.8$ and $\lambda \in (0.3, 5)$.

### 3.2 Lyapunov Exponent Graphic

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

**Definition 1.** [23]:

Suppose $X$ is a set. The mapping $f : X \to X$ is chaotic in $X$, if $f$ is sensitive to initial conditions, $f$ is topologically transitive, and its periodic points are dense in $X$.

A function $f$ is chaotic if its Lyapunov Exponent is positive.

The Lyapunov Exponent equation is defined as

$$ h(x_j) = \lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} \ln |f'(x_j)| $$  \hspace{1cm} (10)

For this purpose, we need the derivative $f'(x_j)$ from the chaos map, and the derivative from the MSDT map is

$$ (f \circ g)'(x) = \begin{cases} \frac{2r\lambda(1+\lambda(1-2x)^2)-(-4\lambda+8\lambda x)(r^22x)}{(1+\lambda(1-2x)^2)^2}, & 0 \leq x < 0.5 \\ \frac{2r\lambda(1+\lambda(2-2x)^2)-(-8\lambda+8\lambda x)(r\lambda(2x-1))}{(1+\lambda(2-2x)^2)^2}, & 0.5 \leq x < 1 \end{cases} $$  \hspace{1cm} (11)

According to Definition 1, a function is chaotic if its Lyapunov Exponent is positive. Figure 2 shows the graphic of the Lyapunov Exponent of the MSDT Map with $r = 3.8$ based on the following Algorithm 2.
Algorithm 2. Lyapunov Exponent Graphic:
Input : $x_0, \lambda, r$
Output : plot the value of $h(x)$
1. Input initial value, parameter values, number of iterations (n)
2. For $j = 1$ to $n$
3. Calculate $h(x_1)$ according to (10)
4. Plot the value of $h(x)$
5. Next $j$
6. Stop

![Lyapunov Exponent graphic](image)

As seen in Figure 2, for $r \in [1, 4]$, the map has positive Lyapunov Exponents. This means that the MSDT Map is chaotic in that interval.

3.3. NIST Randomness Test
This test is administered to level the randomness of the number sequence generated by the MSDT map as in equation (8). The NIST Test Suite is a statistical pack containing 16 tests developed to test the randomness of binary sequences [24]. Table 1 shows the test results for the MSDT map.

| Type of Test                          | P-Value   | Conclusion   |
|--------------------------------------|-----------|--------------|
| 01. Frequency Test (Monobit)         | 0.73386   | Random       |
| 02. Frequency Test within a Block    | 0.64962   | Random       |
| 03. Run Test                         | 0.06858   | Random       |
| 04. Longest Run of Ones in a Block   | 0.02275   | Random       |
| 05. Binary Matrix Rank Test          | 0.33069   | Random       |
| 06. Discrete Fourier Transform (Spectral) Test | 0.27081   | Random       |
| 07. Non-Overlapping Template Matching Test | 0.66691   | Random       |
| 08. Overlapping Template Matching Test | 0.13058   | Random       |
| 09. Maurer's Universal Statistical test | -1.0      | Non-Random   |
| 10. Linear Complexity Test           | 0.83337   | Random       |
| 11. Serial test:                     | 1.14e-09  | Non-Random   |
|                                      | 0.02930   | Random       |
| 12. Approximate Entropy Test         | 4.89e-15  | Non-Random   |
Table 1 shows that the MSDT chaos map passes most of the NIST randomness test. Therefore, this map is an excellent RNG with randomness quality over 82.4%.

4. Conclusion
The development done by composing the MS Map and the Dyadic Transformation Map successfully generated the chaotic MSDT Map. This is shown by the dense bifurcation diagram and the continuously positive Lyapunov Exponent for $x_0 = 0.6$, $r = 3.8$, and $\lambda = 3.5$, and a level of 82.4% in randomness from the NIST test result.

Acknowledgments
This research is funded by Directorat of research and community engagements Universitas Indonesia in the Hibah PITTA scheme with 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] 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
[3] Eva N and Suryadi MT, (2013). Chaos-Based Encryption Algorithm for Digital Image Proceedings IICMA 169-177
[4] 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
[5] Suryanto Y, Suryadi MT, and Ramli K, (2017). A New Image Encryption using color scrambling based on chaotic permutation multiple circular shrinking and Expanding Multimedia Tools and Applications 76 16831-16854
[6] 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
[7] Laptyeva TV, Flach S and Kladko K, (2011). The weak password problem: Chaos, criticality, and encrypted p-CAPTCHAs EPL 95 981-981
[8] Shu Jun L and Xuan Z, (2002). Cryptanalysis of a chaotic image encryption method International Symposium on Circuits and System 2 87-91
[9] Qinan L, (2011). Color image encryption algorithm and its decryption method protecting from shearing attack Computer engineering and design 32 509-512
[10] Suryadi MT, Nurpeti E, Widya D, (2014). Performance of Chaos-Based Encryption Algorithm for Digital Image TELKOMNIKA 12 675-682
[11] Sun F, Liu S and Li Z, (2008). A novel image encryption scheme based on spatial chaos map Chaos Solitons Fractals 38 631-640
[12] 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
[13] 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
[14] Pareek NK, (2012). Design and Analysis of a Novel Digital Image Encryption Scheme. *International Journal of Network Security & Its Applications* 4, 95-108.

[15] 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.

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

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

[18] 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).

[19] 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*.

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

[21] Suryadi MT, Maria YTI, and Satria Y, (2015). Encryption Algorithm using New Modified map for digital image *Proceedings of IICMA* 71-78.

[22] Suryadi M T, Maria Y T I, and Yudi S, (2016). *New Modified Map for Digital Image Encryption and Its Performance*. The Asian Mathematical Conference 2016 (AMC 2016).

[23] Devaney, R.L, (1989). *An introduction to chaotic dynamical systems* (2nd ed.). Addison-Wesley Publishing company, Inc.

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