A new chaos function development through the combination of Circle map and MS map

Ichsani Mursidah[1], *Suryadi* MT[2,*], and *Sarifuddin* Madenda[1]

[1]Department of Information Technology, Universitas Gunadarma, Depok, 16424, Indonesia
[2]Department of Mathematics, Faculty of Mathematics and Natural Sciences (FMIPA), Universitas Indonesia, Depok 16424, Indonesia

Abstract. Digital data protection is very important to prevent manipulation of digital data by unauthorized parties. Reliable techniques for securing digital data are needed, safe and fast. One technique is to use cryptography. One of the cryptographic techniques that can be used to encode digital data is to use the chaos function. We propose in this paper a new chaos function which is a composition of Circle map and MS map functions. This function has chaotic nature and the result of which is named the MSI-Circle map. The sensitivity and randomness tests of the MSI-Circle map function are carried out using a bifurcation diagram, Lyapunov exponent, and NIST test suites. The analysis result of the bifurcation diagram shows that the MSI-Circle map has a good density at the value of $r \in (-\infty, -3] \cup [3, -\infty]$. Lyapunov exponent has a non-negative value at $x_0 = 0.4, r = 3.8, \Omega = 0.5, \lambda = 2.1, K = 4$ which is the domain $x_n \in (0, 1)$ and parameter values r, Ω, λ and K are any real numbers. The results of the NIST randomness level test show that the MSI-Circle map function passed all the randomness test of 16 NIST tests.

Keywords. Lyapunov exponent, bifurcation diagram, MS map, Circle map, chaos function

1 Introduction

Currently, information and communication technology is developing very rapidly, these developments can be seen easily get information with the internet. The internet is a medium that can make it easier for users to obtain various information and communication processes from anywhere in the world and at any time. Someone can easily send personal data to other people so that the data can be widely spread on the internet.

Personal data that is highly confidential needs to be safeguarded against threats of manipulation or data theft. This is done so that the data is not known by unauthorized parties. Therefore, reliable, safe, and fast security techniques are needed, one of which is cryptography. Cryptography is a mathematical technique related to data or information security issues [1]. There are several encoding methods, namely the Advanced Encryption Standard (AES) algorithm, the Data Encryption Standard (DES) algorithm, and the Rivest-Shamir-Adleman (RSA) algorithm. The digital image encryption algorithm

*Corresponding author: yadi.mt@sci.ui.ac.id

requires a long time and low key space but produces well-encrypted images. However, the preferred digital image encryption is digital image encryption which takes faster time without sacrificing its security [2]. The use of chaos-based image encryption is one solution to the image security problem.

Chaos is a type of system or function behavior that is disorderly, sensitive to initial values, parameters, and ergodic. A chaotic function is a function that has chaotic properties. The chaos function has proven to be very useful for data protection [3]. Two well-known chaos functions that exhibit chaotic properties are MS map and Circle map, where Circle map and MS map have high randomness potential.

The Circle map is a one-dimensional map that maps a circle onto itself. Circle map is also very difficult to attack from a brute force attack because it has an advantage with an entropy value of 7.99 with the lowest correlation close to zero and a key space of up to $10^{3\times17}$. Correlation close to zero and entropy close to 8 are important parameters for good image encryption [4].

MS map is a modification of Logistic map which produces an average encryption time which is relatively the same as the average decryption time. The MS map function is resistant to known plaintext attacks because the encrypted image has a uniform distribution. Key sensitivity level reaches 10^{-17}, very secure against brute force attacks. With a key space of up to 3.24×10^{634} [5, 6].

Currently, many researchers are using and producing new chaos maps that are applied to the digital data encryption process [4–12, 14–25]. Referring from the previous results, specifically that uses the Circle map and MS map. This research a new function that is chaotic is developed through the composition of the MS map and Circle map functions. This function is used as a random keystream generator.

2 Research method

The Circle map is a one-dimensional function that maps a circle to itself [4], having the equation,

$$f(x) = \left(x + \Omega + \frac{K}{2\pi}\sin(2\pi x)\right) \bmod 1 \tag{1}$$

with $n = 0, 1, 2, 3, \ldots$, initial value $x_0 \in (0, 1)$, and Ω, K are any real numbers with $a \mod 1$ defined as,

$$a \mod 1 = a - \lfloor a \rfloor \tag{2}$$

The MS map function is a function obtained from the modification of the chaos Logistic map function [5, 6]. This function is shown below,

$$g(x) = \frac{\lambda r x_n}{1 + \lambda (1 - x_n)^2} \pmod 1 \tag{3}$$

with $n = 0, 1, 2, 3, \ldots$, $x_0 \in (0, 1)$, and parameter values $\lambda, r \in \mathbb{R}$.

The proposed new chaos function is develop through the composition process of the two chaos functions in Equation (1) and (3). The composition of the MS map and Circle map functions as a new chaos function is expressed as a function $h(x)$ in Equation (5).

$$h(x) = (g \circ f)(x) \tag{4}$$

$$h(x) = \frac{\lambda r \left[\left(x + \Omega + \frac{K}{2\pi}\sin(2\pi x)\right) \bmod 1\right]}{1 + \lambda \left(1 - \left[\left(x + \Omega + \frac{K}{2\pi}\sin(2\pi x)\right) \bmod 1\right]\right)^2} \pmod 1 \tag{5}$$

and can be written as the recursion,

$$x_{n+1} = \frac{\lambda r\left[\left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) \bmod 1\right]}{1 + \lambda\left(1 - \left[\left(x_n + \Omega + \frac{K}{2\pi}\sin(2\pi x_n)\right) \bmod 1\right]\right)^2} \pmod 1 \tag{6}$$

We name the new recursion as MSI-Circle map.

3 Results and discussion

The MSI-Circle map function is also a chaotic function which can be demonstrated based on analysis of bifurcation diagrams and Lyapunov exponents. In addition, concerning the randomly generated number sequence, the randomness test was carried out using 16 NIST randomness tests [26].

3.1 Bifurcation diagram

A bifurcation diagram shows the value approximated by the stability of the periodic points of a function due to changes in parameter values. Bifurcation diagrams are diagrams that occur as a result of changes in a dynamical system as a function of the parameters in the system. If the bifurcation points on the bifurcation diagram are dense, then the function is chaotic [1]. Algorithm 1 shows the logical flow of the bifurcation diagram calculation process and the results of this diagram display are shown in Fig. 1.

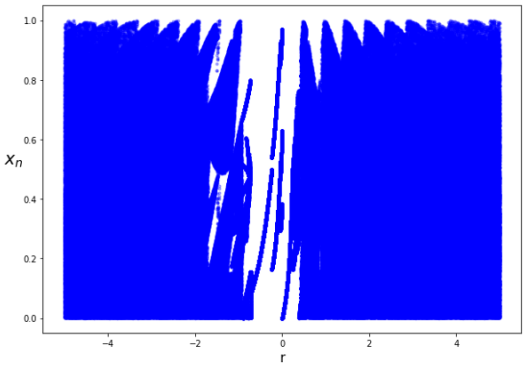

Fig. 1. MSI-Circle map bifurcation diagram parameter of r.

Seen in Fig. 1, the results of the bifurcation diagram are dense for $r \in (-\infty, -3] \cup [3, -\infty]$. Hence, MSI-Circle map function is chaotic in that interval.

Seen in Fig. 2 through Fig. 4, bifurcation diagram parameter of λ, Ω, and K are dense, this means that the parameter values in that area are very random and the number is very large which will be used as key values to generate the MSI-Circle map function's key stream.

3.2 Lyapunov exponent

The Lyapunov exponent of a dynamical system is the rate of separation of any two infinitesimally close trajectories [15]. Chaotic function can be seen from the dependence on sensitivity to initial values and parameters, which can be calculated with the Lyapunov

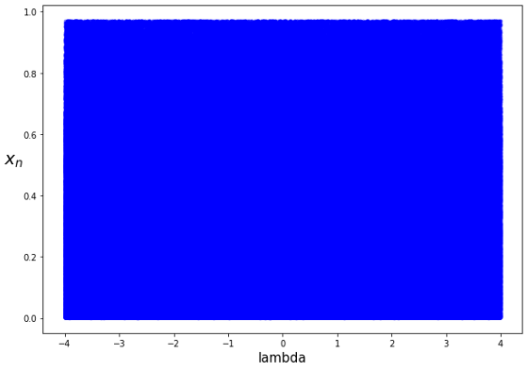

Fig. 2. MSI-Circle map bifurcation diagram parameter of λ.

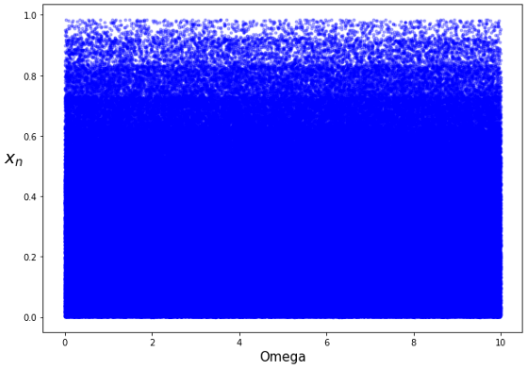

Fig. 3. MSI-Circle map bifurcation diagram parameter of Ω.

exponent [3]. The positive Lyapunov exponent indicates that the new chaos function is a dynamic system and the chaotic properties are better [26]. The Lyapunov exponential equation is defined according to Equation (7):

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n} ln \left| f' \left(x_j \right) \right| \tag{7}$$

The results of the calculation of the Lyapunov value are presented in the form of a graph as shown in Fig. 5-8.

As seen in Fig. 5, the Lyapunov exponent shows a positive value at the value of $r \in [0.4, 4]$. It can be said that the MSI-Circle map function is chaotic in that interval.

As seen in Fig. 6, the Lyapunov exponent shows a positive value at the value of $\lambda \in [0.1, 3]$. This means, the MSI-Circle map function is chaotic.

The Lyapunov exponent shows in Fig. 7, positive value of $\Omega \in [0, 1) \cup [1.1, 4]$. It can be said that the MSI-Circle map function is chaotic in that interval.

The Lyapunov exponent shows in Fig. 8, positive value of $K \in [0, 4]$. It can be said that the MSI-Circle map function is chaotic in that interval. Based on the bifurcation diagram and Lyapunov exponent, we can find intervals that are domains that can be selected as initial values and parameters for building chaotic keystreams.

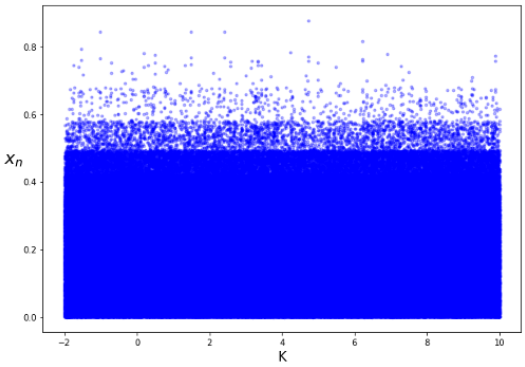

Fig. 4. MSI-Circle map bifurcation diagram parameter of K.

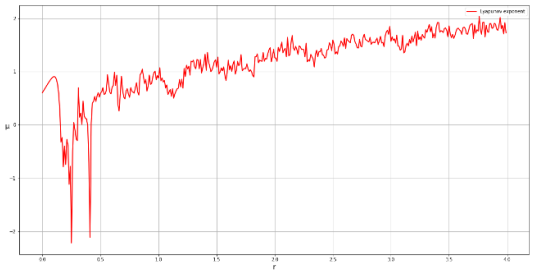

Fig. 5. Lyapunov exponent parameter r of the MSI-Circle map.

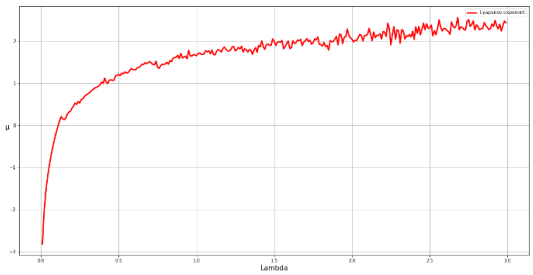

Fig. 6. Lyapunov exponent parameter λ of the MSI-Circle map.

3.3 NIST randomness test

To see the level of randomness of the sequence of random numbers generated from the chaos function MSI- Circle map according to Equation (5). Tests were carried out using the NIST randomness test. NIST Test Suite is a statistical package consisting of 16 tests developed to test the randomness of a sequence of random numbers in the form of binary values [24]. The test results are presented in Table 1.

Table 1 shows that the MSI-Circle map passed all NIST randomness tests. So it can be said that the MSI-Circle map function is a random number generator function with excellent randomness properties, reaching 100 %.

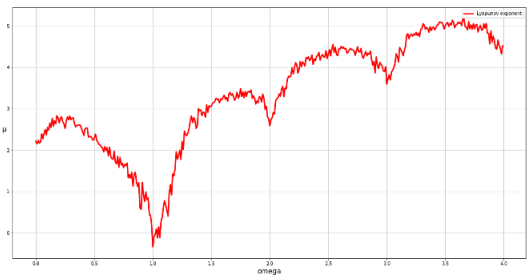

Fig. 7. Lyapunov exponent parameter Ω of the MSI-Circle map.

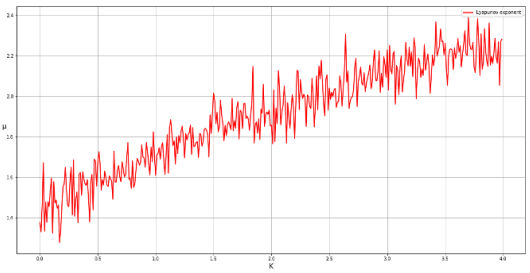

Fig. 8. Lyapunov exponent parameter K of the MSI-Circle map.

Table 1. NIST Randomness Test Result of the MSI-Circle map

Type of Test	P-Value	Conclusion
Frequency Test (Monobit)	0.1378089205910381	Random
Frequency Test within a Block	0.8476988583858784	Random
Run Test	0.8777689456322431	Random
Longest Run of Ones in a Block	0.5619840183848979	Random
Binary Matrix Rank Test	0.5201621952939345	Random
Discrete Fourier Transform (Spectral) Test	0.9341778199756322	Random
Non-Overlapping Template Matching Test	0.11454848936970671	Random
Overlapping Template Matching Test	0.14793005479093957	Random
Maurer's Universal Statistical Test	0.7065355312495885	Random
Linear Complexity Test Serial	0.6928878429130652	Random
Serial Test	0.4795679645403097	Random
	0.814744388811974	Random
Approximate Entropy Test	0.7439705495984551	Random
Cumulative Sums (Forward) Test	0.04751851410116755	Random
Cumulative Sums (Reserve) Test	0.25500776056476404	Random
Random Excurcions Test	0.5673568276662320	Random
Random Excurcions Varian Test	0.6580912761789920	Random

4 Conclusion

The development of a new chaos function, through the function composition method between MS map and Circle map, has been successfully carried out. The new chaos function is

declared as the MSI-Circle map function. The developed MSI-Circle map function is also chaotic. It can be seen from the results of the bifurcation diagram that it is solid for the value of $r \in (-\infty, -3] \cup [3, -\infty]$. The Lyapunov exponent value is always non-negative for the value of $r \in [0.4, 4]$. The level of randomness reached 100 % of the results of the NIST randomness test for the value of $x_0 = 0.4, r = 3.8, \Omega = 0.5, \lambda = 2.1, K = 4$. Compared to the SIYu map, the MSI-Circle map function can be said to be better because the NIST randomness test shows that the chaotic SIYu map has a randomness level of 62.5 %.

Acknowledgements

This research is funded by Ministry of Education and Culture with contract No. 155/e5/PG.02.00.PT/2022.

References

1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography* (CRC press, 2018).
2. N .K. Pareek, V. Patidar, and K. K. Sud, Image Vis. Compu. **24**, 926 (2006)
3. L. Kocarev and S. Lian, *Chaos-based cryptography: Theory, algorithms, and applications*, Vol. 354 (Springer Science & Business Media, 2011).
4. R. Premnath, S. Arumugam, S. Rethinam, C. Lakshmi, and A. Rengarajan, IEEE **2019**, 1-5 (2019).
5. M. Suryadi, Y. Maria, and Y. Satria, *Proceedings of IICMA*, 2015, pp. 71-78.
6. M. Suryadi, M. Y. T. Irsan, and Y. Satria, J. Phys. Conf. Ser. **893**, 012050 (2017).
7. S. B. Kembaren, S. Suryadi, and T. Triswanto, *Prosiding Seminar Nasional & Internasional*, 2018, Vol. 1.
8. E. Nurpeti, Suryadi, *Proceedings of IICMA*, 2014, pp. 169-177.
9. Y. Suryanto, Suryadi, K. Ramli, in *Multimedia Tools and Applications* (Springer, 2017).
10. M. Suryadi, Y. Satria, and M. Fauzi, J. Phys. Conf. Ser. **974**, 012028 (2018).
11. Y. Satria, M. Suryadi, I. M. Solihat, L. N. Prawadika, and I. M. Sholihat, J. Phys. Conf. Ser. **1490**, 012046 (2020).
12. M. Suryadi, Y. Satria, V. Melvina, L. N. Prawadika, and I. M. Sholihat, J. Phys. Conf. Ser. **1490**, 012024 (2020).
13. M. Suryadi, Y. Satria, and L. N. Prawadika, J. Phys. Conf. Ser. **1490**, 012045 (2020).
14. M. Suryadi, Y. Satria, A. Hadidulqawi, J. Phys. Conf. Ser. **1821**, 012037 (2021)
15. Y. Satria, M. Suryadi, and D. Cahyadi, J. Phys. Conf. Ser. **1821**, 012035 (2021).
16. R. H. Prayitno, S. A. Sudiro, and S. Madenda, *Sixth International Conference on Informatics and Computing (ICIC)*, 2021, pp. 1-6.
17. B. K. Yakti, S. Madenda, S. A. Sudiro, and P. Musa, *Sixth International Conference on Informatics and Computing (ICIC)*, 2021, pp. 1-7.
18. F. Sun, S. Liu, Z. Li, and Z. Lu, Chaos Solitons & Fractals **38**, 631–640 (2008).
19. Y. Zhang, F. Zuo, Z. Zhai, and C. Xiaobin, International Symposium on Electronic Commerce and Security (IEEE, 2008), 347–350.
20. S. Li and X. Zheng, International Symposium on Circuits and Systems (IEEE, 2002), Vol. 2, 87-91.
21. J. Ahmad and F. Ahmed, *International Journal of Video and Image Processing and Network Security (IJENS)*, 2012, pp. 18-31.
22. X. Wu, H. Kan, J. Kurths, in *Applied Soft Computing* (Elsevier, 2015), pp. 24–39.

23. Z. Tang, et al., Secur. Commun. Netw. 2019, 8694678 (2019)
24. Rukhin, et al., in *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (National Institute of Standards and Technology, 2001).
25. M. Makmun, S. Suryadi, and S. Madenda, International Journal of Video and Image Processing and Network Security (IJAIR, 2012), Vol. 9, 267–270.
26. R. Devaney, in *An introduction to chaotic dynamical systems* (CRC Press, 2018).