A New Chaos Function Developed through the Composition of the MS Map and the Circle Map

Ichsani Mursidah[1, a)] Suryadi[2,b)] Sarifuddin Madenda[1] Suryadi Harmanto[1]

[1]*Department of Information Technology, Universitas Gunadarma, Depok, 16424, Indonesia*
[2] *Department of Mathematics, Universitas Indonesia, Depok 16424, Indonesia*
[a)] Corresponding author: mursidah@staff.gunadarma.ac.id
[b)]yadi.mt@sci.ui.ac.id

Abstract. The rise of digital data theft makes researchers try to find better methods for digital data protection. Confidential digital data can be secured by encryption methods, one of which is the chaos function. We propose in this paper a new chaos function which is a composition of MS Map and Circle Map functions. This function has chaotic nature and is named the MS Circle Map. The sensitivity and randomness tests of the MS Circle map function are carried out using a bifurcation diagram, Lyapunov Exponent, and NIST. The analysis result of the bifurcation diagram shows that the MS Circle map has a good density at the value of $r \in (0,4)$. Besides that, the Lyapunov Exponent has a non-negative value at $r \in [0.4, 4]$, $x_0 = 0.9,\ r = 3.8,\ \Omega = 0.5\ \lambda = 2.1$ which is the domain $x_n \in (0, 1)$ and parameter values r, λ, and Ω, K are any real numbers. The results of the NIST randomness level test show that the MSC Map function all passed the randomness test of 16 NIST tests.

INTRODUCTION

Information and communication technology continues to overgrow and it is effortless for internet users to obtain various data and information from any part of the world at any time. Information can be in the form of text, images, audio, and video. Therefore, a reliable, safe, and fast data security technique is needed. One of them is the application of cryptography related to information security aspects such as confidentiality, data integrity, entity authentication, and originating data authentication.[1]

Cryptography is divided into two parts, namely classical cryptography and modern cryptography. Classical cryptography prioritizes the secrecy of the algorithm used, while modern cryptography prioritizes the secrecy of the encryption key. There are several cryptographic methods including using the Data Encryption Standard (DES) algorithm, the Advanced Encryption Standard (AES) algorithm and the Rivest-Shamir-Adleman (RSA) algorithm. Encryption of data by these three types of algorithms requires a long computation time and low key space even though it produces good encrypted data. Currently, there is a need for faster digital data and information encryption methods without compromising security [2]. The solution to this need is a chaos function-based encryption method. This method provides a good combination of aspects of speed, high security, and complexity.

Many digital image encryption techniques have been studied, including is chaos-based data encryption techniques. Chaos function has random properties, is sensitive to initial values and parameters, and is ergodic. The chaos function has been proven to be very suitable for keystream generation in data encryption[1].

Many chaos functions have been applied by researchers in the digital data image process [2-20]. The chaos function can also be used as a random number generator (RNG). In addition, a random number generator (RNG) can also be generated from a combination of two or more chaos functions [21-22]. This is done to increases security from various attacks when the chaos function is used for digital image encryption.

The main problem of this research is how to develop a new chaos function which has much higher encryption security performance. The idea of developing this new chaos function is through the composition of two chaos functions MS Map and Circle Map which will produce one new chaos function.

Two chaos functions that are known to exhibit chaotic properties are MS Map [23- 24] and Circle Map [25], where Circle Map and MS Map have a high potential for randomness. In this paper, a new chaos function will be developed which is the result of the composition of the MS Map chaos function with the Circle Map chaos function. The result of the composition is a new function which is also chaotic. So that the new function can be used as a choice as a function of generating random numbers that are chaotic.

The new chaos function's chaotic behaviour will be quantitatively analyzed based on bifurcation diagrams, Lyapunov Exponent, and randomness tests with the National Institute of Standard Technologies Tests (NIST). The analysis results are the basis for considering whether the new chaos function can be implemented in cryptography.

METHOD

The MS map function is the result of the development of the logistic map function [23-24]. This function is shown in equation (1)

$$x_{n+1} = \frac{r\lambda x_n}{1+\lambda(1-x_n)^2} \ mod\ 1 \tag{1}$$

with $n = 0,1,2,3, \dots$, initial value $x_0 \in (0,1)$, and parameter values $r \in (0,4)$, $\lambda \in (0,4)$ and $x\ mod\ 1 = x - \lfloor x \rfloor$.

The Circle Map is a one-dimensional function that maps a circle to itself [6]. The Circle Map function is defined as equation (2)

$$x_{n+1} = \left(x_n + \Omega + \frac{K}{2\pi} sin(2\pi x_n)\right) mod\ 1 \tag{2}$$

with $n = 0,1,2,3, \dots$, initial value $x_0 \in (0,1)$, and Ω, K are any real numbers, where Ω can be limited at $0 \leq \Omega < 1$.

The proposed new chaos function is develop through the composition process of the two chaos functions in equation (1) and (2), in the following method:

1. Express the Circle Map function in equation (2) as a function of f(x);
2. Express the MS Map function in equation (1) as a function of g(x);
3. The compositional form of the function g(x) to f(x) is defined as equation (3);
4. Do the algebraic process of equation (3) and produce a new chaos function h(x) as equation (4). Furthermore, the function h(x) is expressed as an MS Circle Map function which has 5 parameters, namely $x_n \in (0,1)$ and parameter values $r \in (0,4)$, $\lambda \in (0,4)$, and Ω, K are any real numbers, where Ω can be limited at $0 \leq \Omega < 1$ with $n = 0,1,2,3, \dots$

$$h(x) = (f \circ g)(x) \tag{3}$$

$$h(x) = \left(\left(\frac{r\lambda x_n}{1+\lambda(1-x_n)^2} mod\ 1 + \Omega + \frac{K}{2\pi} sin\left(2\pi\left(\frac{r\lambda x_n}{1+\lambda(1-x_n)^2} mod\ 1\right)\right)\right) mod\ 1\right) \tag{4}$$

RESULT

The MS Circle Map function which was developed through the composition process of the MS Map and Circle Map functions is also a chaos function. This can be shown by the bifurcation diagram and the Lyapunov exponent. In addition, concerning the randomly generated number sequence, the randomness test was carried out using 16 NIST randomness tests [26].

Here, the initial value and parameters of the MS Circle map used for the test is $x_0 = 0.9, r = 3.8, \lambda = 2.1, \Omega = 0.5, K = 1000$.

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. The bifurcation diagram can tell if a function is chaotic. 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 Figure 1.

Algorithm 1. Bifurcation Diagram

Input: x_0 , λ , $\Omega, K,$ and r

Output: plots of x_n

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

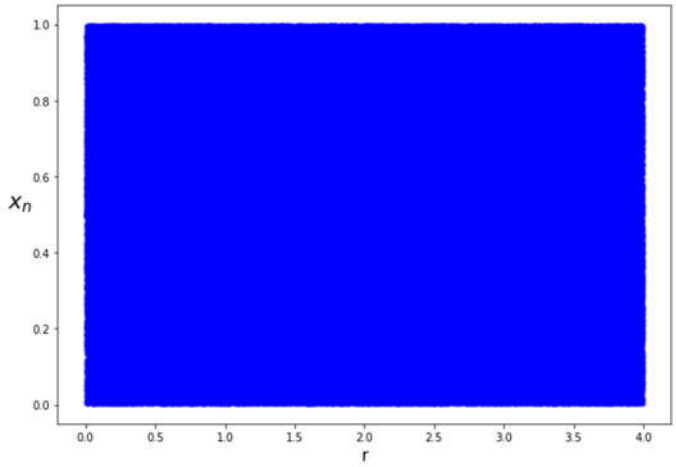

FIGURE 1. MS Circle Map Bifurcation Diagram

Seen in Figure 1, the results of the bifurcation diagram are dense for $\boldsymbol{r} \in (\mathbf{0}, \mathbf{4})$. Hence, MS Circle map function is chaotic in that interval.

Lyapunov Exponent

Referring to [1], the chaotic function can be seen from the dependence on sensitivity to initial values and parameters, which can be calculated with the Lyapunov exponent. The positive Lyapunov exponent indicates that the new chaos function is a dynamic system and the chaotic properties are better. [27] The Lyapunov exponential equation is defined according to equation (5):

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{n} ln\left|f'(x_j)\right| \tag{5}$$

The derivative of the MS Circle map can be seen in equation (6) below.

$$h'(x) = -\lambda r \frac{\lambda x^2 - \lambda - 1}{(\lambda x^2 - 2\lambda x + \lambda + 1)^2} \left\{1 + 2\Omega \cos\left[2\Omega\left(\frac{r\lambda x}{1+\lambda(1-x_n)^2}\right)\right]\right\} \quad (6)$$

The lyapunov exponent value of the MSC Map is calculated using Algorithm 2. The results of the calculation of the lyapunov value are presented in the form of a graph as shown in Figure 2.

Algorithm 2. Lyapunov Exponent Graphic

Input: $x_0, \lambda, \Omega, K,$ and r

Output: plot the value of μ

1. Input initial value, parameter values, number of iterations (n)
2. For j=1 to n
   3. Calculate μ according to (5)
   4. Plot the value of μ
5. Next j
6. Stop

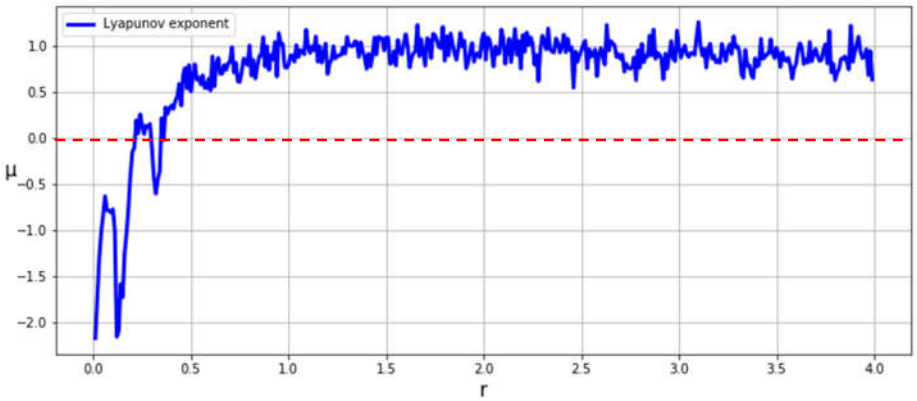

FIGURE 2. Lyapunov Exponent of the MS Circle Map

As seen in Figure 2, the Lyapunov exponent shows a positive value at the value of $r \in [0.4, 4]$. It can be said that the MS Circle map function is chaotic in that interval.

NIST Randomness Test

To see the level of randomness of the sequence of random numbers generated from the chaos function MS Circle map according to equation (4). 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 [26]. The test results are presented in Table 1.

TABLE 1. NIST Randomness Test Result of the MS Circle Map

Type of Test	P-Value	Conclusion
Frequency Test (Monobit)	0.977662	Random
Frequency Test within a Block	0.567429	Random
Run Test	0.356528	Random

Longest Run of Ones in a Block	0.743168	Random
Binary Matrix Rank Test	0.622197	Random
Discrete Fourier Transform (Spectral) Test	0.335273	Random
Non-Overlapping Template Matching Test	0.735657	Random
Overlapping Template Matching Test	0.500748	Random
Maurer's Universal Statistical Test	0.816673	Random
Linear Complexity Test Serial	0.353947	Random
Serial Test	0.521116	Random
	0.706375	Random
Approximate Entropy Test	0.900518	Random
Cumulative Sums (Forward) Test	0.838476	Random
Cumulative Sums (Reserve) Test	0.813864	Random
Random Excurcions Test	0.505771*	Random
Random Excurcions Varian Test	0.254903*	Random

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

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 MS Circle Map function. The developed MSC map function is also chaotic. It can be seen from the results of the bifurcation diagram that it is solid for the value of $r \neq 0$. 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 $x_0 = 0.9, r = 3.8, \lambda = 2.1, \Omega = 0.5, K = 1000$.

ACKNOWLEDGEMENTS

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

REFERENCES

1. Kocarev,L., Lian, S. Chaos-based cryptography: Theory, algorithms, and applications. Springer: Verlag, Berlin, 2011;pp. 1-25.
2. Pareek NK,. Design and Analysis of a Novel Digital Image Encryption Scheme International Journal of Network Security & Its Applications 4,2012. 95-108
3. Kembaren, S; Suryadi, Triswanto, Implementasi Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi Komposisi Logistic dan Gauss Iterated Map , Seminar Nasional Edusainstek ISBN: 978-602-5614-35-4, 2018.
4. Nurpeti, E., and Suryadi. Chaos-Based Encryption Algorithm for Digital Image Proceedings IICMA 2013. 169-177.
5. Suryanto Y, Suryadi, and Ramli K,. A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding Journal of Information Hiding and Multimedia Signal Processing, 2016. 7 697-713.
6. Suryadi, Satria,Y., and Fauzi, M. "Implementation of digital image encryption algorithm using logistic function and DNA encoding." Journal of Physics: Conference Series. Vol. 974. No. 1. IOP Publishing, 2018.
7. Satria, Y., Suryadi, Solihat, I.M., Prawadika, L.N., and Melvina, V. "The composition of the improved logistic map and the MS map in generating a new chaotic function." Journal of Physics: Conference Series. Vol. 1490. No. 1. IOP Publishing, 2020.
8. Suryadi, M., Satria, Y., Melvina, V., Prawadika, L.N., and Solihat, I.M. "A new chaotic map development through the composition of the MS Map and the Dyadic Transformation Map." Journal of Physics: Conference

Series. Vol. 1490. No. 1. IOP Publishing, 2020
9. Suryadi, M. T., Satria, Y., and Prawadika, L. N. "An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination." Journal of Physics: Conference Series. Vol. 1490. No. 1. IOP Publishing, 2020.
10. Suryadi, M. T., Satria, Y., and Hadidulqawi, A. "Implementation of the Gauss- Circle Map for encrypting and embedding simultaneously on digital image and digital text." Journal of Physics: Conference Series. Vol. 1821. No. 1. IOP Publishing, 2021.
11. Satria, Y., M. T. Suryadi, and Cahyadi, D. "Digital text and digital image encryption and steganography method based on SIYu map and least significant bit." Journal of Physics: Conference Series. Vol. 1821. No. 1. IOP Publishing, 2021.
12. Prayitno, R.H., Sudiro, S. A., and Madenda, S, "Avoiding Lookup Table in AES Algorithm," 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1-6, doi: 10.1109/ICIC54025.2021.9632897.
13. Yakti, B.K., Madenda, S., Sudiro, S.A., and Musa, P. "Processing Speed Comparison of the Least Significant Bit (LSB) Steganography Algorithm on FPGA and Matlab," 2021 Sixth International Conference on Informatics and Computing (ICIC), 2021, pp. 1-7, doi: 10.1109/ICIC54025.2021.9632978.
14. Makmun, Suryadi, Madenda, S. A New Chaotic Map Development Through the Composition of the Logistic Map and Circle Map. International Journal of A Advance and Innovative Research. **9**, 2 p. 267-270, 2022.
15. 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
16. Sun F, Liu S and Li Z, (2008). A novel image encryption scheme based on spatial chaos map Chaos Solitons Fractals **38** 631-640
17. 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
18. Shujun L and Xuan Z, (2002). Cryptanalysis of a chaotic image encryption method International Symposium on Circuits and System **2** 87-91
19. Qinan L, (2011). Color image encryption algorithm and its decryption method protecting from shearing attack Computer engineering and design 32 509-512
20. 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
21. Wu, X., kana, H., and Kurths, J. A new color image encryption scheme based on DNA sequence and multiple Improved 1D chaotic maps. Applied soft computing **37**, pp. 24-39.
22. Zhenjun Tang ,Ye Yang, Shijie Xu, Chunqiang Yu , and Xianquan Zhang. Image Encryption with Double Spiral Scans and Chaotic Maps. Hindawi Security and Communication Networks. (2019)
23. Suryadi , Irsan, M.Y.T., and Satria, Y. Encryption Algorithm using New Modified map for digital image Proceedings of IICMA,2015.pp: 71-78
24. Suryadi, Irsan, M.Y.T., and Satria,Y. New Modified Map for Digital Image Encryption and Its Performance. The Asian Mathematical Conference 2016 (AMC 2016).
25. Premnath,L., Arumugham,S., Rethinam, S., Lakshmi, S., and Rengarajan, A, "Performance Evaluation of Chaotic Maps & Attractors in Image Encryption," 2019 International Conference on Computer Communication and Informatics (ICCCI), 2019, pp. 1-5, doi: 10.1109/ICCCI.2019.8822032.A.
26. Rukhin, J. Soto, j. Nechvatal, E. Barker, S. Leigh, A Statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special publication 2010
27. Devaney, R.L. An Introduction to chaotic dynamical systems. (Addison-Wesley Publishing company, Inc., 1989)