TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 24, No. 1, February 2026, pp. 228∼239
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i1.27551

New chaos function from the composition of DTM and Gauss iterated map for digital image encryption

Adrianus Yosia, Tokonyai Tawanda Jonathan Rabvemhiri, Suryadi MT
Department of Mathematics, Faculty of Mathematics and Sciences, Universitas Indonesia, Depok, Indonesia

Article Info

Article history:

Received Sep 15, 2025
Revised Nov 14, 2025
Accepted Dec 8, 2025

Keywords:

Composition
Dyadic transformation map
Dyadic transformation-Gauss iterated map
Gauss iterated map
New chaos function

ABSTRACT

This manuscript introduces a novel chaotic discrete function, formulated through the composition of the dyadic transformation map (DTM) and the Gauss iterated map (GIM), and designated as DTGIM. The National Institute of Science and Technology (NIST) randomness test suite, bifurcation diagrams, and Lyapunov exponents are used to examine the chaotic characteristics of DTGIM. With initial condition $x_0 = 0.12345$ and parameters $\alpha = -15$ and $\beta = 0.3$, the function shows chaotic behavior in the bifurcation diagram and produces a positive Lyapunov exponent. Strong randomness is further confirmed by NIST tests, which achieve 100% for 32-bit binary sequences and 63.75% for 8-bit binary sequences. Additionally, we compare a number other chaotic discrete functions that also employ the composition method. These findings show that DTGIM is a viable option for applications involving chaos-based cryptography.

Corresponding Author:

Adrianus Yosia
Department of Mathematics, Faculty of Mathematics and Sciences, Universitas Indonesia
Depok, Indonesia
Email: adrianus.yosia@ui.ac.id

1. INTRODUCTION

This age can be seen as the age of information exchange. The utilization of information technology makes the trade of data easier. Information can be formed as text, images, audio, or video, which are commonly used today. Yet, the dawn of technological information is also followed by security issues. As a precaution to it, application of cryptography is needed to ensure confidentiality, data integrity, entity authentication, or originating data authentication [1]-[3].

Cryptography itself is generally acknowledged as the best method of data protection against passive and active fraud [4]. At least there are two divided camps of cryptography: classical cryptography and modern cryptography [1]. Classical cryptography focuses on the confidentiality of the algorithm that is being used, while modern cryptography concentrates on the secrecy of the encryption key [1]. Currently, the demand for having faster digital data and information encryption methods with uncompromising security is rising [5]. One of the solutions to answer the problem is a chaos function-based encryption method. This article also wants to contribute to the development of chaos-function-based.

There are various implementations of the chaos function-based encryption method [6]-[12]. Also, there are various functions that have chaotic properties, such as circle maps, logistic maps, modified sine (MS) maps, tent maps, Gauss maps, dyadic transformation maps (DTM), Henon maps, Nahrain maps, sine–iterative Yu (SIYu), and others [7]-[14]. Also, various methods are used to improve the effectiveness and chaotic behavior of chaotic function such as sequential method [6], modification [8], composition [15], or multi-dimensional method [16]. As an illustration (the idea is from [13]), see the Figure 1. Before continuing this article into our main purpose, as an addition, the implementation of chaos-based function encryption itself can be used in engineering [17], [18], medical field [19]-[24], IOT [25]-[31], or satellite image encryption [32]-[34].

Figures 1(a) to (c) serve as an illustration on the method's diversity. Our aim is to define the new chaos function using composition (see Figure 1(c)). Regarding the research gap for our work, there are several papers that discuss on creating a new chaos functions using composition method especially for DTM and Gauss iterated map (GIM). Until today, the work that has done is the composition of MS map and DTM [1], GIM and dyadic transformation [13]. In this paper, we will explore the composition from DTM and GIM. Also, as a comparison, we will also find the same route for DTM and GIM. As an addition, we will compare our work with other work that using composition method.

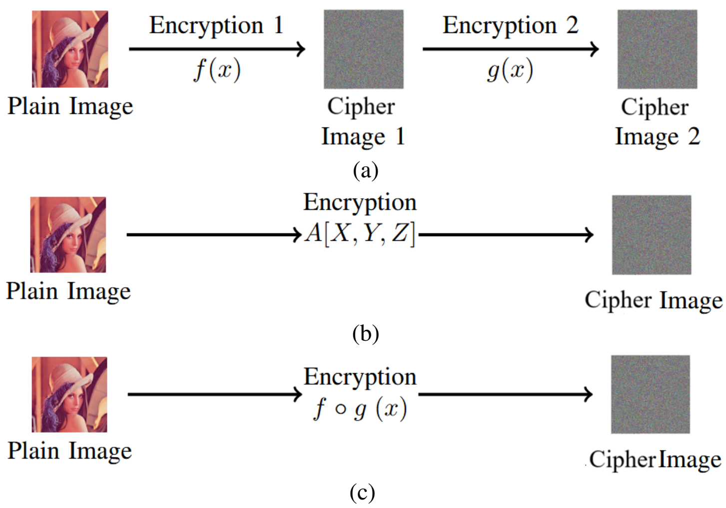


Figure 1. The method for making a new chaos function, we using Lena.jpeg (512×512); (a) improving chaos function through sequential method [15], (b) improving chaos function through multidimensional map [16], and (c) improving chaos function through composition [13]

2. METHOD

In this section, we will discuss on how we deal with four things in this article: the chaos functions, the bifurcation diagram, the Lyapunov exponent, and also the National Institute of Science and Technology (NIST) test.

- The composition of two chaos function

  The method that we will use to improve the chaos function is composition of two chaos function [1], [6], [13]. The first function is the dyadic transformation function or Bernoulli function [35] that can be defined as:

$$f(x) = 2x \bmod 1 \tag{1}$$

$$= \begin{cases} 2x, & 0 \leq x < 0.5 \\ 2x - 1, & 0.5 \leq x < 1 \end{cases} \tag{2}$$

Meanwhile, the Gauss iterated function [2], [13] is defined as:

$$g(x) = \exp(-\alpha x^2) + \beta \tag{3}$$

where $\alpha, \beta \in \mathbb{R}$. Then, using the composition of two functions method between (2) and (3), the new function is, as we called it, the dyadic transformation-Bernoulli function, which can be seen (4):

$$f \circ g\ (x) = \begin{cases} \left[2\exp(-\alpha x^2) + 2\beta\right] \bmod 1 & , 0 \leq x < 5 \\ \left[2\exp(-\alpha x^2) + (2\beta - 1)\right] \bmod 1 & , 0.5 \leq x < 1. \end{cases} \tag{4}$$

Now, transforming the function into the discrete map function [3], where $f \circ g\,(x_n) = x_{n+1}$, the (4) can be transformed as (5):

$$x_{n+1} = \begin{cases} \left[2\exp(-\alpha x_n^2) + 2\beta\right] \mod 1 & , 0 \leq x_n < 0.5, \\ \left[2\exp(-\alpha x_n^2) + (2\beta - 1)\right] \mod 1 & , 0.5 \leq x_n < 1, \end{cases} \quad (5)$$

for $n \in \mathbb{Z}^+$. We will call the (5) DTGIM. As a brief note here, the addition $\mod 1$ is to make sure that $0 \leq x_n \leq 1$.

- Bifurcation diagram
  The bifurcation diagram is a graphical tool that describes stability and nonlinear behavior from the chaos function based on the changing of parameters [36]-[38]. Then, the chaotic behavior can be described from the bifurcation diagram [39]. We use this Algorithm 1 below for finding the bifurcation diagram.
- Lyapunov exponent
  The Lyapunov exponent is a value that can trace the chaos from the system [37]. In our article, following [8], we will find the best Lyapunov exponent for a certain parameter. First, the Lyapunov exponent can be found by using this calculation:

$$\text{Lyapunov exponent (LE)} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |h'(x_i)| \quad (6)$$

  when LE < 0, the system tends to be stable, while LE > 0, it has chaotic behavior [38]. As a brief note, the function $h'(x_i)$ is the derivation from a chaos function $h(x)$. In this paper, the chaos function $h(x)$ is the function DTGIM on (5), also GIM and DTM. In this article, we will find the best Lyapunov exponent by using the algorithm from [8]. We use Algorithms 2 and 3 for finding the best Lyapunov. Both of the algorithms will be used in one picture for the sake of effectiveness.
- NIST test result
  We will use the NIST testing suite [40] to examine the randomness of the DTGIM function. The NIST testing suite consists of 15 statistical tests (with 16 results) for displaying the randomness of a chaos function. We will use the Python implementation from Steven Ang for our testing [41]. Also, for testing the file, we will generate 8-bit and 32-bit for testing the binary data (follow the idea from [8], [42]). In addition, we will observe the calculation of entropy and autocorrelation to strengthen our result [38], [43], [44].

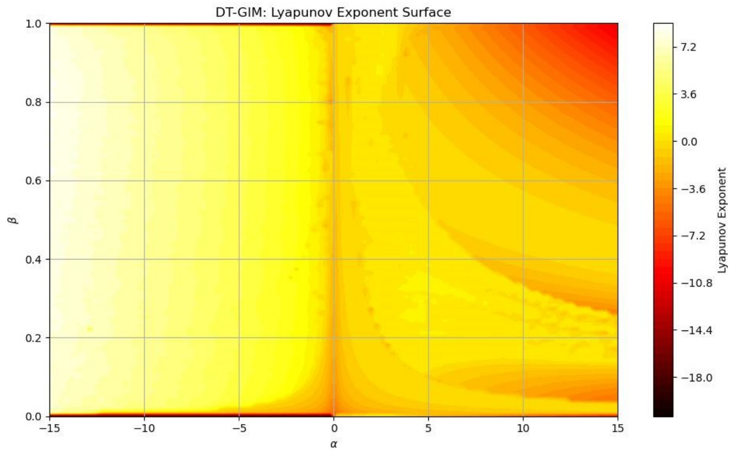
Algorithm 1. Bifurcation diagram
Input : x_0, α, and β
Output : Plot of x_n values
1. Input initial values and parameter and number of iterations (i)
2. For $n = 1$ to i:
    3. Calculate x_n based on the chaos function.
    4. Plot the value of x_n
5. Next n
6. Stop

Algorithm 2. Lyapunov exponent graphic:
Input : x_0, α, and β
Output : Plot the value of $h(x)$
1. Input initial values and parameter and number of iterations (j)
2. For $n = 1$ to j:
    3. Calculate $h(x_j)$ based on the chaos function
    4. Plot the value of $h(x)$
5. Next j
6. Stop

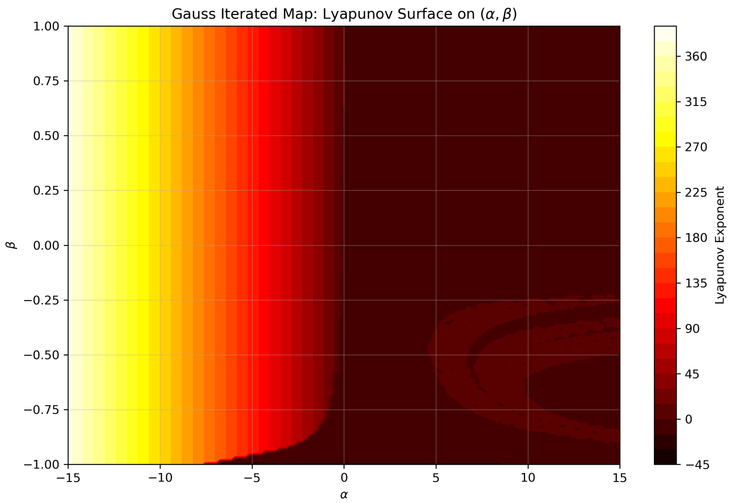
Algorithm 3. Highest Lyapunov exponent:
Input : x_0, α, and β
Output : Highest Lyapunov Exponent
1. Input initial values and parameter and number of iterations (i), parend
2. While parameter $<$ parend:
    2.1. If $h'(x) < 10^{-15}$,
        Lyapunov Exponent = $-\infty$
    end if
    else
        2.1.1. sum = 0
        2.1.2. for $i = 0$ to $n - 1$
            2.1.2.1. sum = sum + $h'(x)$
            2.1.2.2. sum = sum/n
    2.2. parameter = parameter +stepsize
3. Find the Highest Lyapunov Exponent
4. Stop

3. RESULTS AND DISCUSSION

We will start the discussion from the Lyapunov surface plot (heatmap; see Figure 2) from parameter α, β, and Lyapunov exponent (see (6)) from the chaos map at (5) and also the GIM. Since dyadic transformation has no parameter, then there is no Lyapunov surface plot from it. From Figure 2(a), regarding DT-GIM, the value of LE is dominantly positive when $\alpha < -10$, whenever $\beta \in (0, 1]$. Then, the great candidate of α and β can be seen when $\alpha < -10$. We will choose $\alpha = -15$ and $\beta = 0.3$ as the parameter for DTGIM. Next, Figure 2(b) shows that the value of LE is dominantly positive when $\alpha < -10$, whenever $\beta \in (-1, 1)$. Then, we will use $\alpha = 7.3$ and $\beta = -0.6$ for GIM (see also [45]). The picture was created by us using Python. The brighter the color, the higher the probability that the system will become chaotic.



(a)

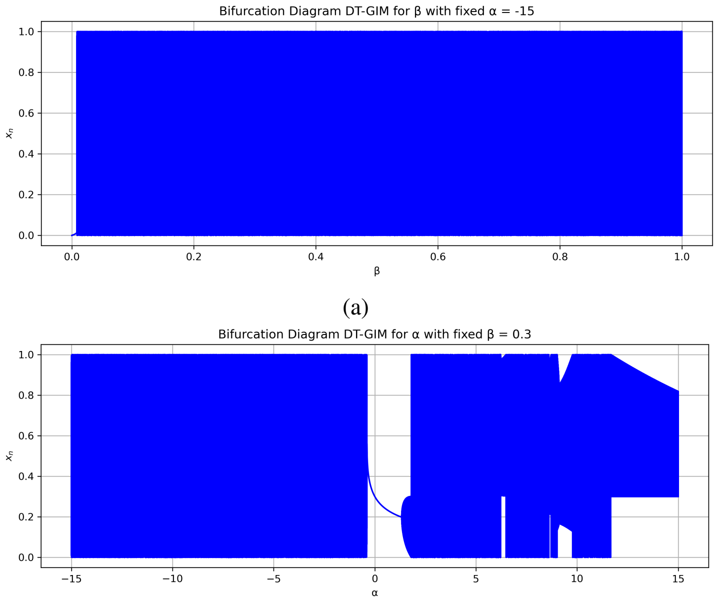


(b)

Figure 2. Lyapunov surface from DT-GIM and GIM; (a) Lyapunov surface plot from DT-GIM for $\beta \in [0, 1]$ and seed $x_0 = 0.12345$ and (b) Lyapunov surface plot from GIM for $\alpha \in [-15, 15]$, $\beta \in [0, 1]$ and seed $x_0 = 0.12345$

3.1. Bifurcation diagram

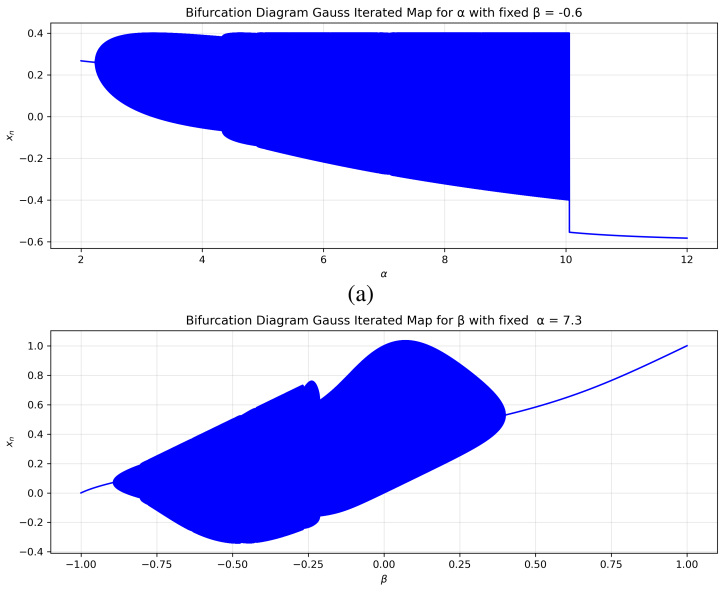
Now, following our finding from Figure 2, we will find the bifurcation diagram of DTGIM for $\alpha = -15$, $\beta = 0.3$ and seed $x_0 = 0.12345$ (see [6]) and the results are in Figure 3. From Figure 3, we can see that the DTGIM is dense when $\alpha = -15$ (Figure 3(a)) and $\beta = 0.3$ (Figure 3(b)). Hence, it shows a great result for the parameter. For GIM, following the recommendation from Figure 2, we will show the Bifurcation diagram of GIM for $\alpha = 7.3$ and $\beta = -0.6$ for seed $x_0 = 0.12345$. The result is in Figure 4. From Figure 4, we will use parameter $\alpha = 10$ (Figure 4(a)) and $\beta = -0.6$ (Figure 4(b)) because it gives a great result for the parameter. Since the DTM in our case does not have parameters, then we will not show the result here.



(a)

(b)

Figure 3. Bifurcation diagram for DT-GIM function; (a) the diagram for fixed $\alpha = 15$ for $\beta \in [-1, 1]$ and (b) the diagram for fixed $\beta = 0.3$ for $\alpha \in [-20, 20]$. The pictures were created by us using Python



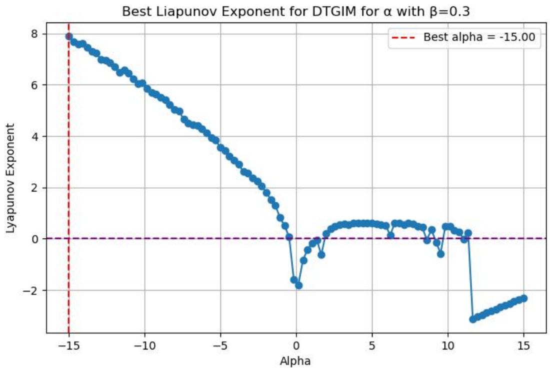
(a)

(b)

Figure 4. Bifurcation diagram for GIM; (a) the diagram for fixed $\beta = -0.6$ and (b) the diagram for fixed $\alpha = 7.3$

3.2. Lyapunov exponent

Once more, following our finding from Figure 2, we will explore the value of the Lyapunov exponent for $\alpha = -15$ and $\beta = 0.3$ for $x_0 = 0.12345$ using Algorithms 2 and 3 [6], [26]. Then, the plot of the Lyapunov exponent and the best value of it will be shown by Figure 5. From the calculation that has been shown in Figure 5, the Lyapunov exponent is positive for $\alpha < -1$ on the function DTGIM. Also, following Algorithm 3, it shows that $\alpha = -15$ is the highest (best) parameter for $\beta = 0.3$ (Figure 5(a)). From the same picture, the best Lyapunov exponent of GIM is achieved for $\beta = -0.6$ is when $\alpha = 7.3$ (Figure 5(b)). Since dyadic transformation gives a constant in its derivative, the Lyapunov exponent gives the constant result and a positive one $(\ln 2)$ for every seed.



(a)

(b)

Figure 5. The Best Lyapunov exponent; (a) the diagram for DTGIM with fixed $\beta = 0.3$ and (b) the diagram for GIM with fixed $\beta = -0.6$

3.3. NIST test result

In this section, we will show the NIST test results for three chaos functions, that is DT, GIM, and DTGIM. After we show the result. Now, for the binary file (8-bit and 32-bit), we use this step to create the binary file (see [45]):

- Choose parameter values, in our case $\alpha = -15$ and $\beta = 0.3$.
- Take an initial value for our case $x_0 = 0.12345$ and record all the map's values for 127000 iterations (for 8-bit) and 33250 (for 32-bit) and remove the first 2000 iterations.
- Transform the value into integers that range from 0 to 255 (for 8-bit) and 0 to $2^{32} - 1$ (for 32-bit).
- Transform all of the integers into 8-bit (or 32-bit) binary strings
- Concatenate all the strings to form a 1000000-bit file and input it into the NIST test.
- The test will decide the randomness.

We show the NIST result test for 8-bit and 32-bit binary that can be seen in Table 1 (in Appendix). As a brief description, Table 1 will show the randomness of the chaos function either for DTGIM, DTM, or GIM for a certain parameter. We will add the randomness percentage to show the randomness. Also, as an addition, we will also show the entropy per word and bit to show the utilization of randomness from the data. Also, the autocorrelation plot is shown to support the description of randomness of our problem. The three additions will be a support to strengthen the NIST test result.

3.4. Comparison with other chaos function with composition

Lastly, our interest goes into comparison with other functions that use the composition method. As for comparison with other data, we can see from the results of other researchers that utilize either GIM or DTM that composition is a method for creating a new chaos function. From the latest research, at least there are four other candidates besides our work [1], [6], [13], [45]. Table 2 shows the comparison between our work and theirs.

Table 2. The comparison between chaos functions that use composition as a method

	DTGIM	MS-CM [1]	GIM-DT [13]	GM-CM [45]	MS-DT [6]
Lyapunov exponent mean	8.2334	13.7329	8.0308	8.2	3.069
NIST pass percentage	100% (32 bit) 62.5% (8 bit)	100%	100%	25% (8-bit)	82.4%
Number of pixels change rate (NPCR) (%)	99.622	99.5984	99.5514	99.4214	99.6521
Unified average changing intensity (UACI) (%)	33.1144	33.5008	33.7116	27.2815	33.6363
Mean entropy (bits)	7.968	7.9868	7.9458	7.7544	7.9874

3.5. Discussion

Our first finding, the result from Lyapunov Surface (Figure 2), Bifurcation diagram (Figures 3 and 4), Lyapunov exponent (Figure 5) and NIST result (Table 1) shows a consistent result. In the case of DTGIM, the parameter $\alpha = -15$ and $\beta = 0.3$ gives the best result for 62.5% randomness (8-bit data) and 100% (32-bit data). For the 8-bit data, the entropy per word shows that almost all of the possible numbers from 1-255 has been explored by DTGIM, yet the result is 62.5% at best. Regarding the test itself, the NIST test proceeded smoothly. This fact is shown by the autocorrelation picture from the 8-bit and 32-bit. We also try different seeds (not shown here), and for 32-bit data, DTGIM still gives 100% randomness, and the same for 8-bit. The entropy per bit and per word shows that there is so much room to explore since DTGIM has a high randomness. Therefore, DTGIM shows a strong candidate for a chaos function.

Next, Table 1 shows the comparison between DTGIM and two other functions prior to composition. For GIM and DTM, the result also shows that both of the functions still lack randomness, comparing them with DTGIM. Of course, the problem with GIM is that the parameter that we have chosen still does not utilize the full potential of GIM. Yet, at least for our research, we conclude that DTGIM is far superior with our parameter. We also try different seeds, and it still gives the same result (not shown here). For DTM, the result is the same for both 8-bit and 32-bit, since the nature of the function is "only shifting" the number. Hence, the results show a very weak randomness from our research. The result, in line with the observation regarding chaotic function, has a low entropy [46]. Therefore, comparing DTGIM, GIM, and DTM, our research shows that the new chaos function surpasses its functions prior to composition.

From Table 2, we conclude that in general, the image encription from the four functions gives a great result since the Lyapunov exponent mean is positive. It means that all four functions show a highly chaotic behavior. Also, high rating of NPCR and UACI shows that all of the function is a great chaos functions. In terms of rating, our research is second after the composition of MS-map and circle map. Therefore, we can say that DTGIM is one of the good chaos function candidates.

4. CONCLUSION

We have explored the possibility of a new chaos function that we construct from the composition of dyadic transformation and GIM. From the result, we show that DTGIM has a chaotic behavior from the Lyapunov exponent, bifurcation diagram, and also NIST test result for $\alpha = -15$ and $\beta = 0.3$. We also compare DTGIM with GIM and DTM. The result is satisfying and shows that DTGIM is superior to its predecessor prior to composition. Therefore, as the purpose of this article, we conclude that DTGIM is one of the good chaos functions. For the future trajectories of this research, improving the randomness for the NIST test on 8-bit binary data by using another technique for generating random numbers is a viable one. Also, for the DTGIM itself, room for improvement can still be made since the entropy report shows that we only cover at least 40% random numbers at 32-bit data. Similar to this issue, GIM has great randomness also. We suggest that one can use negative α. One can also move to apply the chaos function to encrypting and decrypting the image for the next project. Lastly, another route can be taken for comparing the result with other methods of chaotic function and analyzing the difference.

FUNDING INFORMATION

The authors state no funding was involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Adrianus Yosia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Tokonyai Tawanda Jonathan Rabvemhiri		✓				✓		✓	✓	✓	✓	✓		✓
Suryadi MT	✓		✓	✓		✓	✓	✓	✓		✓		✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [initials: AY], upon reasonable request.

REFERENCES

[1] I. Mursidah, S. Suryadi, S. Madenda, and S. Harmanto, “A New Chaos Function Developed through the Composition of the MS Map and the Circle Map,” *Research Transformation and Digital Innovation on Mathematics Education*, 2023.

[2] D. Solev, P. Janjic, and L. Kocarev, “Introduction to chaos,” in *Studies in Computational Intelligence*, vol. 354, 2011, pp. 1–25, doi: 10.1007/978-3-642-20542-2_1.

[3] L. Kocarev, “Chaos-based cryptography: A brief overview,” *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001, doi: 10.1109/7384.963463.

[4] Mishkovski and L. Kocarev, “Chaos-Based Public-Key Cryptography,” in *Studies in Computational Intelligence*, vol. 354, 2011, pp. 27–65, doi: 10.1007/978-3-642-20542-2_2.

[5] N. K Pareek, “Design and Analysis of a Novel Digital Image Encryption Scheme,” *International Journal of Network Security & Its Applications*, vol. 4, no. 2, pp. 95–108, Mar. 2012, doi: 10.5121/ijnsa.2012.4207.

[6] MT. Suryadi, Y. Satria, V. Melvina, L. N. Prawadika, and I. M. Sholihat, “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, p. 012024, Jun. 2020, doi: 10.1088/1742-6596/1490/1/012024.

[7] Y. Satria, MT. Suryadi, and D. J. Cahyadi, “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, p. 012035, Mar. 2021, doi: 10.1088/1742-6596/1821/1/012035.

[8] MT. Suryadi, M. Y. T. Irsan, and Y. Satria, “New modified map for digital image encryption and its performance,” *Journal of Physics: Conference Series*, vol. 893, p. 012050, Oct. 2017, doi: 10.1088/1742-6596/893/1/012050.

[9] MT. Suryadi, Y. Satria, and M. Fauzi, “Implementation of digital image encryption algorithm using logistic function and DNA encoding,” *Journal of Physics: Conference Series*, vol. 974, p. 012028, Mar. 2018, doi: 10.1088/1742-6596/974/1/012028.

[10] Y. Suryanto, Suryadi, and K. Ramli, “A secure and robust image encryption based on chaotic permutation multiple circular shrinking and expanding,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 4, pp. pp. 697-713, 2016.

[11] MT. Suryadi, E. Nurpeti, and D. Widya, “Performance of chaos-based encryption algorithm for digital image,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 7, no. 4, pp.697-713, Sep. 2014, doi: 10.12928/TELKOMNIKA.v12i3.106.

[12] Y. Dai and X. Wang, “Medical image encryption based on a composition of Logistic Maps and Chebyshev Maps,” in *2012 IEEE International Conference on Information and Automation, ICIA 2012, IEEE*, Jun. 2012, pp. 210–214, doi: 10.1109/ICInfA.2012.6246810.

[13] M. Mudrika, S. Mt, and S. Madenda, “New chaos function of composition function Gauss map and dyadic transformation map for digital image encryption,” *ITM Web of Conferences*, vol. 61, p. 01004, Jan. 2024, doi: 10.1051/itmconf/20246101004.

[14] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.

[15] J. S. Armand Eyebe Fouda, J. Yves Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 3, pp. 578–588, Mar. 2014, doi: 10.1016/j.cnsns.2013.07.016.

[16] Sahay and C. Pradhan, "Multidimensional comparative analysis of image encryption using gauss iterated and logistic maps," in *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, 2017, pp. 1347–1351, doi: 10.1109/ICCSP.2017.8286603.

[17] G. Chen, "Controlling Chaos and Bifurcations in Engineering Systems," Boca Raton, FL, USA: CRC Press, 1999.

[18] K. W. Wong, B. S. H. Kwok, and W. S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 15, pp. 2645–2652, Apr. 2008, doi: 10.1016/j.physleta.2007.12.026.

[19] S. K. Naveenkumar, H. T. Panduranga, and Kiran, "Chaos and Hill Cipher Based Image Encryption for Mammography Images," in *ICIIECS 2015 - 2015 IEEE International Conference on Innovations in Information, Embedded and Communication Systems, IEEE*, Mar. 2015, pp. 1–5, doi: 10.1109/ICIIECS.2015.7193175.

[20] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[21] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9907–9927, Apr. 2017, doi: 10.1007/s11042-016-3585-x.

[22] S. Mostafa, M. A. N. I. Fahim and A. B. M. A. Hossain, "A new chaos based medical image encryption scheme," *2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT)*, 2017, pp. 1-6, doi: 10.1109/ICIEV.2017.8338573.

[23] S. Ibrahim et al., "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[24] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast Reaching Finite Time synchronization Approach for Chaotic Systems with Application in Medical Image Encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021, doi: 10.1109/ACCESS.2021.3056037.

[25] Boutros, S. Hesham, and B. Georgey, "Hardware acceleration of novel chaos-based image encryption for IoT applications," in *2017 29th International Conference on Microelectronics (ICM), IEEE, Dec. 2017*, pp. 1–4, doi: 10.1109/ICM.2017.8268833.

[26] S. Nath, S. Som, and M. Negi, "LCA approach for Image Encryption Based on Chaos to Secure Multimedia Data in IoT," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, IEEE, Nov. 2019, pp. 410–416, doi: 10.1109/ISCON47742.2019.9036311.

[27] J. Jain, A. Jain, S. K. Srivastava, C. Verma, M. S. Raboaca, and Z. Illés, "Improved Security of E-Healthcare Images Using Hybridized Robust Zero-Watermarking and Hyper-Chaotic System along with RSA," *Mathematics*, vol. 10, no. 7, p. 1071, Mar. 2022, doi: 10.3390/math10071071.

[28] M. Stanciu and O. Datcu, "Atmel AVR microcontroller implementation of a new enciphering algorithm based on a chaotic generalized Hénon map," in *2012 9th International Conference on Communications, COMM 2012 - Conference Proceedings*, IEEE, Jun. 2012, pp. 319–322, doi: 10.1109/ICComm.2012.6262554.

[29] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller," *Microprocessors and Microsystems*, vol. 45, pp. 297–309, Sep. 2016, doi: 10.1016/j.micpro.2016.06.004.

[30] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller," *Microprocessors and Microsystems*, vol. 56, pp. 1–12, Feb. 2018, doi: 10.1016/j.micpro.2017.10.013.

[31] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels," *Chaos, Solitons and Fractals*, vol. 133, p. 109646, Apr. 2020, doi: 10.1016/j.chaos.2020.109646.

[32] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 326–337, Jul. 2010, doi: 10.1016/j.camwa.2009.12.033.

[33] Y. Bentoutou, E. H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Advances in Space Research*, vol. 66, no. 1, pp. 176–192, Jul. 2020, doi: 10.1016/j.asr.2019.09.027.

[34] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite Time Chaos Synchronization in Time-Delay Channel and Its Application to Satellite Image Encryption in OFDM Communication Systems," *IEEE Access*, vol. 9, pp. 21332–21344, 2021, doi: 10.1109/access.2021.3055580.

[35] D. J. Driebe, Fully Chaotic Maps and Broken Time Symmetry, vol. 4, no. 1. in *Nonlinear Phenomena and Complex Systems*, vol. 4. Dordrecht: Springer Netherlands, 1999, doi: 10.1007/978-94-017-1628-4.

[36] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering, Third Edition*. Boca Raton: Chapman and Hall/CRC, 2024, doi: 10.1201/9780429398490.

[37] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, p. 2585, Jun. 2023, doi: 10.3390/math11112585.

[38] Y. Sun and W. Wang, "Role of image feature enhancement in intelligent fault diagnosis for mechanical equipment: A review," *Engineering Failure Analysis*, vol. 156, p. 107815, Feb. 2024, doi: 10.1016/j.engfailanal.2023.107815.

[39] S.-N. Chow and J. K. Hale, Methods of Bifurcation Theory, vol. 251. in *Grundlehren der mathematischen Wissenschaften*, vol. 251. New York, NY: Springer New York, 1982, doi: 10.1007/978-1-4613-8159-4.

[40] Rukhin, J. Soto, and J. Nechvatal, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *Gaithersburg*, MD, 2010, doi: 10.6028/NIST.SP.800-22r1a.

[41] S. K. Ang, "Stevenang/randomness testsuite." Accessed: Jun. 04, 2025. [Online]. Available: https://github.com/stevenang/randomness testsuite

[42] W. K. S. Tang and Y. Liu, "Formation of high-dimensional chaotic maps and their uses in cryptography," *Studies in Computational Intelligence*, vol. 354, pp. 99–136, 2011, doi: 10.1007/978-3-642-20542-2_4.

[43] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 281–288, Mar. 2001, doi: 10.1109/81.915385.

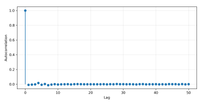
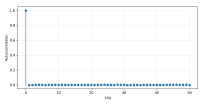
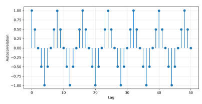
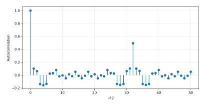
[44] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-based random number generators - Part II: Practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 3, pp. 382–385, Mar. 2001, doi: 10.1109/81.915396.

[45] Suryadi, Y. Satria, and L. N. Prawadika, "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, p. 012045, Mar. 2020, doi: 10.1088/1742-6596/1490/1/012045.

[46] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A Survey on True Random Number Generators Based on Chaos," *Discrete Dynamics in Nature and Society*, vol. 2019, pp. 1–10, Dec. 2019, doi: 10.1155/2019/2545123.

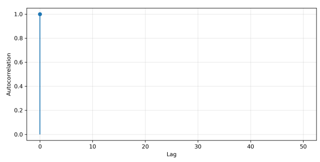
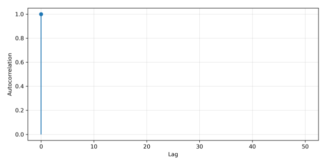
APPENDIX

Table 1. The comparison between the NIST result for 8-bit and 32-bit binary data for the function DT-GIM. The seed that has been used for the test is $x_0 = 0.12345$

Test name	DTGIM (8-bit, $\alpha = -15, \beta = 0.3$) p-value (conclusion)	DTGIM (32-bit, $\alpha = -15, \beta = 0.3$) p-value (conclusion)	GIM (8-bit, $\alpha = 7.3, \beta = -0.6$) p-value (conclusion)	GIM (32-bit, $\alpha = 7.3, \beta = -0.6$) p-value (conclusion)
The frequency (monobit) test	1.77×10^{-14} (non-random)	0.990 (random)	83×10^{-5} (non-random)	0 (non-random)
Frequency test within a block	0.9775 (random)	0.942 (random)	1 (random)	0 (non-random)
The runs test	0 (non-random)	0.2661 (random)	0 (non-random)	0 (non-random)
Test for the longest-run-of-ones in a block	0.16157 (random)	0.730 (random)	4.4×10^{-220} (non-random)	7.5×10^{-95} (non-random)
The binary matrix rank test	0.29361 (random)	0.111 (random)	0 (non-random)	0 (non-random)
The discrete fourier transform (spectral) test	0.0444 (random)	0.039 (random)	0 (non random)	0 (non-random)
The non-overlapping template matching test	0.54874 (random)	0.614 (random)	0 (non-random)	1.884×10^{-214} (non-random)
The overlapping template matching test	0.12514 (random)	0.131 (random)	0 (non-random)	6.94×10^{-168} (non-random)
Maurer's "universal statistical" test	0.37994 (random)	0.102 (random)	0 (non-random)	0 (non-random)
The linear complexity test	0.64399 (random)	0.651 (random)	0 (non-random)	0 (non-random)
The serial test	0 (non-random)	0.250 (random)	0 (non-random)	0 (non-random)
	0 (non-random)	0.660 (random)	0 (non-random)	0 (non-random)
The approximate entropy test	0 (non-random)	0.033 (random)	0 (non-random)	0 (non-random)
The cumulative sums (cusums) test (forward)	3.15403×10^{-14} (non-random)	0.498 (random)	0 (non-random)	0 (non-random)
The cumulative sums (cusums) test (backward)	1.781×10^{-14} (non-random)	0.508 (random)	0.0165 (non-random)	0 (non-random)
The random excursions test	0.54972* (random)	0.452* (random)	$1.4 \times 10^{-6*}$ (non-random)	0.982* (random)
The random excursions variant test	0.6250* (random)	0.496* (random)	0.903* (random)	0.0601* (random)
Randomness percentage	$\frac{10}{16} \times 100\% = 62.5\%$	$\frac{16}{16} \times 100\% = 100\%$	$\frac{2}{16} \times 100\% = 12.5\%$	$\frac{2}{16} \times 100\% = 12.5\%$
Entropy per word	7.977 (out of 8)	14.931 (out of 32)	0.0816 (out of 8)	13.114 (out of 32)
Entropy per bit	0.997064	0.4666	0.0102	0.409
Autocorrelation				

* Accumulation of several values

Table 1. The comparison between the NIST result for 8-bit and 32-bit binary data for the function DT-GIM. The seed that has been used for the test is $x_0 = 0.12345$ *(continued)*

Test name	DTM (8-bit) p-value (conclusion)	DTM (32-bit) p-value (conclusion)
The frequency (monobit) test	0 (non-random)	0 (non-random)
Frequency test within a block	0 (non-random)	0 (non-random)
The runs test	0 (non-random)	0 (non-random)
Test for the longest-run-of-ones in a block	4.4×10^{-220} (non-random)	4.4×10^{-220} (non-random)
The binary matrix rank test	0 (non-random)	0 (non-random)
The discrete fourier transform (spectral) test	0 (non-random)	0 (non-random)
The non-overlapping template matching test	0 (non-random)	0 (non-random)
The overlapping template matching test	0 (non-random)	0 (non-random)
Maurer's "universal statistical" test	0 (non-random)	0 (non-random)
The linear complexity test	0 (non-random)	0 (non-random)
The serial test	0 (non-random)	0 (non-random)
	0 (non-random)	0 (non-random)
The approximate entropy test	0 (non-random)	0 (non-random)
The cumulative sums (cusums) test (forward)	0 (non-random)	0 (non-random)
The cumulative sums (cusums) test (backward)	0 (non-random)	0 (non-random)
The random excursions test	$2.9 \times 10^{-12}*$ (non-random)	$2.9 \times 10^{-12}*$ (non-random)
The random excursions variant test	1^* (random)	1^* (random)
Randomness percentage	$\frac{1}{16} \times 100\% = 6.25\%$	$\frac{1}{16} \times 100\% = 6.25\%$
Entropy per word	0 (out of 8)	0 (out of 32)
Entropy per bit	0	0
Autocorrelation		

* Accumulation of several values

BIOGRAPHIES OF AUTHORS

Adrianus Yosia earned a Bachelor of Science in Mathematics from Bandung Institute of Technology. After earning a Master of Theology from Southeast Asia Theological Seminary in Indonesia and Wesley Theological Seminary in Washington, D.C., USA, he worked as a secondary math teacher. He is presently pursuing his M.Sc. in Mathematics at the University of Indonesia in Indonesia (2024). He is also a part of the teaching, learning, and curriculum staff of Citra Kasih School in Indonesia. He is currently interested in dynamic systems and differential partial equations. Furthermore, he is intrigued by the conversation between the fields of mathematics and theology. He can be contacted at email: adrianus.yosia@citrakasih.sch.id, adrianus.yosia@ui.ac.id.

Tokonyai Tawanda Jonathan Rabvemhiri received the B.Sc. degree in Mathematics and Statistics from Zimbabwe Open University, Zimbabwe, in 2022, and the B.Sc. Special Honours degree in Mathematics from Great Zimbabwe University, Zimbabwe, in 2023. He is currently pursuing the M.Sc. degree in Mathematics at the University of Indonesia, Indonesia (2024–2026). His current research interests include mathematical modeling and computational intelligence. He can be contacted at email: rabvemhirittj@gmail.com, tokonyai.tawanda@ui.ac.id.

Suryadi MT received the B.Sc. degree in Mathematics from the Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Indonesia, in 1990, the M.Sc. degree in Informatics Engineering from the Bandung Institute of Technology, Indonesia, in 1998, and the D.Phil. degree from the Department of Electrical and Computer Engineering, Universitas Indonesia, in 2013. He is currently a Professor in the field of Data Security Science at the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia. Currently he is also the head of the research center for cyber-information security and intelligent transportation systems at the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia. He is the author or co-author of more than 50 papers published in prominent international journals and conference proceedings, has written two books, and has contributed a chapter to a book. His current research interests include information security, cryptography, and computational mathematics. He is a member of IndoMS. He can be contacted at email: yadi.mt@sci.ui.ac.id.