New chaos function of composition function Gauss map and dyadic transformation map for digital image encryption

Mudrika Mudrika[1], *Suryadi* MT[2,*], and *Sarifuddin* Madenda[1]

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

Abstract. Encryption algorithms mostly use key-streams generated from random number generators. Several recent studies have shown that the random number generator used is a chaos function. In this paper, a new chaos function will be developed which can be used as a chaotic random number generator. The development is carried out by forming a new chaos function using the function composition method. The function that is composed is the Gauss Map function against the Dyadic Transformation Map. The results of the new chaos function are chaotic, this is based on the results of the analysis obtained from the results of the bifurcation diagram, the Lyapunov Exponent and the National Institute of Standard Technologies Test (NIST) standard randomness test. The results of the bifurcation diagram show that the density is for the value of $\alpha \in [-30,0]$ and has periodic properties to choose the values of $\beta \in [-1.02, -0.75]$, $\beta \in [-0.60, -0.30]$, $\beta \in [0.10, 0.25]$ and $\beta \in [0.55, 0.75]$. A positive value of Lyapunov Exponential diagram will be employed alpha equal to negative value ($\alpha < 0$). The results of the NIST standard randomness test with values $x_0 = 0.9$, $\alpha = -15$ and $\beta = 0.7$ resulted in 100 % passing the test (16 tests).

Keywords. New chaotic, composition, bifurcation, Lyapunov, NIST random test

1 Introduction

In the world of cryptography at this time, there have been many methods and ways to secure data, this is due to the importance of data for being secured and not falling into the hands of irresponsible people in the use of data. To increase safety and good results of cryptography, a unique or complex method is needed.

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

Chaos has three characteristics: sensitivity to initial conditions, random behavior, and it does not have recurring periods. Functions that have chaotic properties are called chaotic functions. Chaos functions have been proven to be very suitable for data protection [1]. Functions that have chaotic properties include Circle maps, Logistic maps, MS maps, Tent maps, Gauss Maps, Dyadic Transformation maps, Henon maps, Nahrain maps, and others [2-13].

In recent years, many encryption algorithms have been implemented. Algorithms such as the DES Algorithm (Data Encryption Standard), AES Algorithm (Advanced Encryption Standard), and RSA (Rivest-Shamir-Adleman) are suitable for text encryption. However, these algorithms are unsuitable for image encryption due to the long time required and high computing power, even though they produce well-encrypted data [14]. What is prioritized in digital image encryption is a faster time without compromising its security. The encryption method for digital images can be fulfilled with chaos-based encryption approaches. This method provides a good combination in terms of speed, a high security and computing power [1].

In the process of encryption and description in a sequential way from two the chaos functions can increase high security but require a long processing time seen in Fig.1.

This sequential method has been used by Yin [7]. The basic idea of this research is to propose a new chaotic function that can maintain a level of security and increase processing time seen in Fig. 2.

In this case, a merger will be proposed by compositions two chaos functions, namely the Gauss Map Function and the Dyadic Transformation Map (GDT), which from this composition will get a new chaos function.

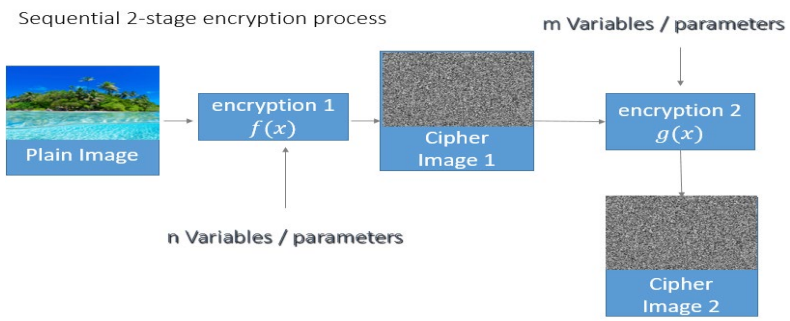

Fig. 1. Encryption process sequential**.**

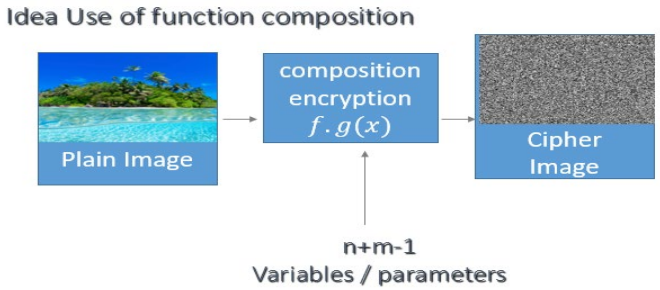

Fig. 2. Process based on function composition

2 Method

In this paper we propose the composition of two chaos functions, Gauss Maps Function and Dyadic Transformation Maps Function. The Gauss Maps Function has a high ability to secure Red Green Blue (RGB) images [12] with the equation shown in Equation (1).

$$f(x) = \exp(-\alpha x^2) + \beta \tag{1}$$

While the Dyadic Transformation Function is a mathematical step function, expressed in the form of Equation (2).

$$g(x) = \begin{cases} 2x, & 0 \le x < 0.5 \\ 2x - 1, & 0.5 \le x < 1 \end{cases} \tag{2}$$

The new Chaos function proposed in this paper is a composition in the form of $f \circ g$ where f is the Gaussian chaos function according to Equation (1), and g chaos is the Dyadic Transformation function in Equation (2), so that the new function looks like Equation (3).

$$(f \circ g)(x) = \begin{cases} \exp(-\alpha(2x)^2) + \beta, & 0 \le x < 0.5 \\ \exp(-\alpha(2x-1)^2) + \beta, & 0.5 \le x < 1 \end{cases} \tag{3}$$

From Equation (3) the recursive form is shown in Equation (4).

$$(f \circ g)(x_{n+1}) = \begin{cases} \exp(-\alpha(2x_n)^2) + \beta, & 0 \le x_n < 0.5 \\ \exp(-\alpha(2x_n-1)^2) + \beta, & 0.5 \le x_n < 1 \end{cases} \tag{4}$$

Furthermore, we can express GDT Map function using Equation (4) as result from the composition of the Gauss chaos function and Dyadic Transformation as shown in Equation (5).

$$(x_{n+1}) = \begin{cases} \exp(-\alpha(2x_n)^2) + \beta, & 0 \le x_n < 0.5 \\ \exp(-\alpha(2x_n-1)^2) + \beta, & 0.5 \le x_n < 1 \end{cases} \tag{5}$$

3 Results

With the results from the analysis of the bifurcation diagram, Lyapunov exponent and the NIST random test consisting of 16 random tests, the GDT Map function generated from the composition between the Gauss chaos function and the chaos Dyadic Transformation function can be said to be as a chaos function.

3.1 Bifurcation diagram

Bifurcation diagram is a diagram that shows an asymptotically approximated value of a system as a function of the parameter in the system. In the bifurcation diagram, it can be seen whether a function is chaotic or not. If the bifurcation diagram contains dense periodic points, the function is said to be chaotic. In determining the value of β, the initial input values are given for $x_0 = 0.9, \beta = -1$ to 1, and $\alpha = 5$.

As seen in Fig. 3, there is a periodic property for its density which is shown in Table 1. In determining the value of β, the initial input values are given for $x_0 = 0.9, \alpha = -30$ to 0, and $\beta = 0.2$.

From the results in Fig. 4, the bifurcation diagram will be dense when the value of alpha (α) -30 to 0, it can be said that the GDT function is chaotic.

Algorithm 1. Bifurcation diagram
Output:
1. Input x_0, α, β, many iterations
2. For t = 1 to iteration
3. Calculate value x_n of the GDT
4. Function
5. Show graph x_n
6. Next t
7. Finish

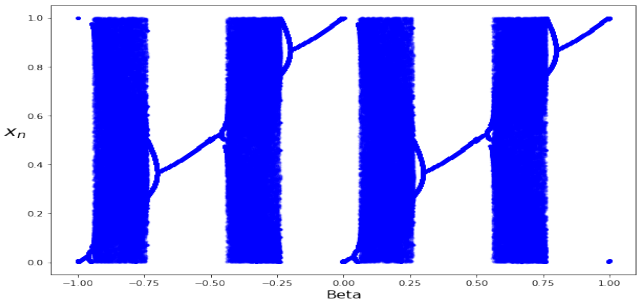

Fig. 3. GDT map bifurcation diagram

Table 1. Density values for the value of Beta (β).

No	Beta value
1	-1.02 to -0.75
2	-0.60 to -0.25
3	0.10 to 0.25
4	0.55 to 0.75

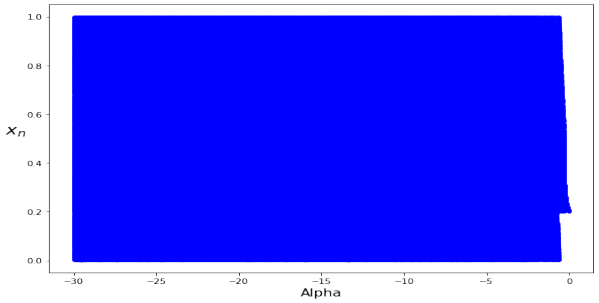

Fig. 4. Bifurcation Diagram of the GDT Map Function with $x_0 = 0.9$, α = -30 to 0, and $\beta = 0.2$.

3.2 Lyapunov exponent diagram

To construct and check global a stability forms a nonlinear system, need the Lyapunov Exponent function, in this case the proposed GDT function is a non-linear system.

The definition of a Lyapunov exponential is:

Let X be a set , f : X → X is a chaos function in X if:

1. f dependence that is sensitive to the initial value
2. f is topologically transitive
3. Periodic points are dense at X

If the value of the Lyapunov exponent is positive, then a function f can be said to be chaotic. The Lyapunov Exponent equation can be expressed in Equation (6).

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{-n} \ln\left|(f^i)'(x_0)\right| \tag{6}$$

Then, takes $(f^i)'$ from Equation (3) to get the result for Equation (7).

$$(f^i)' = \begin{cases} -8\alpha x e^{\alpha(2x)^2}, & 0 \le x < 0.5 \\ -4\alpha(2x-1)e^{\alpha(2x-1)^2}, & 0.5 \le x < 1 \end{cases} \tag{7}$$

The definition says that if the Lyapunov exponent is positive, then a function f can be said to be chaotic. As seen in Fig. 5 that a positive value is generated when the value of alpha is negative, this means to get the GDT function is chaotic if the value alpha (α) of selected is negative.

Algorithm 2. Lyapunov exponent diagram

Output:

1. Input $x_0, \alpha, \beta,$ many iterations
2. For t = 1 to iteration
3. Calculate value μ from Equation (6)
4. Show graph Lyapunov exponent
5. Next t
6. Finish

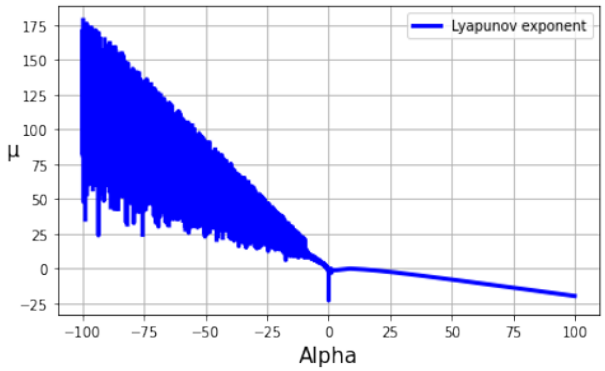

Fig. 5. Lyapunov Exponent Diagram of the GDT Map Function with x_0 = 0.9, β = 0.2 and iter = 100.

Table 2. NIST randomness test results of the GDT chaos function.

Type of Test	P-value	Conclusion
Frequency Test (Monobit)	0.328	Random
Frequency Test within a Block	0.045	Random
Run Test	0.857	Random
Longest Run of Ones in a Block	0.075	Random
Binary Matrix Rank Test	0.277	Random
Discrete Fourier Transform (Spectral) Test	0.748	Random
Non-Overlapping Template Matching Test	0.184	Random
Overlapping Template Matching Test	0.112	Random
Maurer's Universal Statistical test	0.262	Random
Linear Complexity Test	0.158	Random
Serial test:	0.823	Random
	0.946	Random
Approximate Entropy Test	0.110	Random
Cummulative Sums (Forward) Test	0.532	Random
Cummulative Sums (Reverse) Test	0.453	Random
Random Excursions Test	0.471*	Random
Random Excursions Variant Test	0.544*	Random
*Average test score		

3.3 NIST randomness test

NIST Test Suite is a statistical package consisting of 16 randomness tests needed to test a series of random values in binary numbers [15]. From the GDT chaos function in equation (5) to obtain the value of the randomness of the binary number sequence, a randomness test will be carried out using the NIST Random Test, with parameters $x_0 = 0.9$, $\alpha = -15$, and $\beta = 0.7$ and the results are shown in Table 2. The resulting randomness is very good, which is up to 100 %, so the chaos function of the GDT Map can be said to be one of the random number generator functions.

4 Conclusion

A function resulting from the composition of two chaos functions between the Gauss function and the Dyadic Transformation function has succeeded in obtaining a new chaos function and can be used for digital image encryption keystream. This has been proven by various NIST randomness tests which reach 100 % and solid bifurcation diagrams and Lyapunov diagrams which have positive values generated.

References

1. L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory Algorithms and Applications* (Springer, Verlag Berlin Heidelberg, 2011).
2. S. B. Kembaren, S. Suryadi, and T. Triswanto, 2018, *Prosiding Seminar Nasional Pendidikan, Sains dan Teknologi* (Unimus Press, 2018), pp. 263–272.
3. S. Suryadi, Y. Satria, and L. N. Prawadika, J. Phys. Conf. Ser. **1490**, 012045 (2020).
4. S. Suryadi, V. Melina, Y. Satria, L. N. Prawadika, and I. M. Sholihat, J. Phys. Conf. Ser. **1490**, 012024 (2020).
5. S. Suryadi, E. Nurpeti, and D. Widya, Telkomnika **12**, 675–682 (2014).
6. S. Suryadi, M. Y. T. Irsan, and Y. Satria, J. Phys. Conf. Ser. **893**, 012050 (2017).
7. Y. Dai and X. Wang, *Proceeding of the 2012 IEEE International Conference on Information and Automation* (IEEE, 2012), pp. 210–214.
8. A. Sahay and C. Pradhan, *Proceeding of the 2017 International Conference on Communication and Signal Processing* (IEEE, 2017), Vol. **1**, pp. 0015–0018.
9. M. C. Sharma and P. Sharma, Int. J. Comput. Appl. **157**, 18–23 (2017).
10. A. Soleymani, M. J. Nordin, and E. Sundararajan, Sci. World J. **2014**, 536930 (2014).
11. E. Sukirman, S. Suryadi, and M. A. Mubarak, Telkomnika **12**, 651–656 (2014).
12. A. Sahay and C. Pradhan, *Proceeding of the 2017 International Conference on Communication and Signal Processing* (IEEE, 2017), Vol. **1**, pp. 1347-1351.
13. H. A. Abdullah and H. N. Abdullah, Int. J. Wirel. Mob. Comput. **17**, 212–218 (2019).
14. P. K. Naskar and A. Chaudhuri, Int. J. Image Graph. Signal Process. **6**, 30–38 (2014).
15. A. Rukhin et al., *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (NIST, Gaithersburg, 2010).