An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination

Suryadi MT¹, Yudi Satria², Luqman N Prawadika³

¹,²,³Department of Mathematics, Universitas Indonesia, Depok, 16424, Indonesia

E-mail: yadi.mt@sci.ui.ac.id, ysatria@sci.ui.ac.id, nuradip.luqman@yahoo.com

Abstract. Chaos based cryptography has becoming an interesting topic lately, as it utilizes chaotic systems properties for secure key concealment. Many chaotic functions are discovered, constructed, and used time over time for this purpose, which will be our main aim here. Two well known maps that has been known for exhibiting chaotic behaviors are the Gauss Map and the Circle Map, where the Circle Map has unlimited chaos potential, while the Gauss Map's is much weaker and limited. In this paper, we investigate computationally using Python whether the Gauss Map can be improved by combining it with the Circle Map, allowing exploitation of greater chaotic behaviors. For this purpose, an improved version of the Gauss map is constructed, from which, we plot its bifurcation diagrams and Lyapunov exponents graphics, and show that it has a good potential to be a random number generator (RNG) using the NIST test, as these are the three main aspects of chaotic maps utilized in chaos based cryptography. The results obtained from this observation shows that composing the Circle Map into the Gauss Map, along with several manipulations, generates a significantly improved version of the Gauss Map, as it has a bifurcation diagram with much higher density, much higher Lyapunov exponents, and mostly better P-Values from the NIST tests, although it is still not fully suitable for a RNG. The manipulations done here, which aims to conserve the maps ranges to stay within the chaotic intervals and position the Circle Map to be the "variable" of the Gauss Map, allows the chaotic behaviors from the original maps to be bequeathed and strengthened in the new map.

1. Introduction

Data security is an important aspect in modern communication, and greater security is in high demand as technology develops from time to time, including in security breaching. Chaos based cryptography has becoming an interesting topic lately as chaotic systems has a very important property, that is, sensitive dependence on initial conditions [1]. This can be used to conceal keys used in cryptosystems safely, as even a very small shift in the key value will cause a significant difference in the encryption and decryption result, protecting it from brute force attacks. Another appealing property is the random-like behavior, which causes encryption results to have a uniform histogram and a high entropy, protecting it from statistical attacks [2-9]. Considering that it is interesting to analyze whether two chaotic maps can be combined to generate a new map with stronger chaotic behaviors [10-19], here, as a new keystream generator alternative, we will propose a new chaotic map from the well known Gauss Map, which has been investigated by Hemanta [20] to have three types of fractal dimensions, dense bifurcation diagram and positive Lyapunov Exponents at
certain parameter values, and the Circle Map, whose bifurcation diagrams have been sketched by Boyland [21] and show chaotic behaviors. We choose both functions as they have similar value range and the same dimension of one, and for exploratory purposes. Here, we will further analyze both maps specifically in their bifurcation diagrams and Lyapunov Exponents, and use the results to derive an improved version of the Gauss Map which is obtained by combining it with the Circle Map, and eventually conduct an NIST on the modified Gauss Map, which is all done to test whether the resulting new map is suitable to be implemented in cryptography.

2. Research Method
This research is done using three main Python programs, that is, the Lyapunov exponent graphic constructor, the bifurcation diagram constructor, and the NIST randomness test [22], as chaos functions are commonly analyzed computationally [23]. The first two programs are initiated by defining the chaos maps and gathering their plot informations, then adjusting and executing their plot display, and additionally, for the Lyapunov exponent, we seek the parameter value with the highest Lyapunov Exponent. Below is the algorithm for the Lyapunov Exponent calculation based on the formula

\[ \lambda(x_0) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{dx_{n+1}}{dx_n} (n = i) \right| \]

where \( \frac{dx_{n+1}}{dx_n} (n = i) \) is the value of \( \frac{dx_{n+1}}{dx_n} \) evaluated at \( n = i \).

**Algorithm 1. Lyapunov Exponent calculation:**

Input : chaos map, parameter start, parent, number of iterations \( n \), stepsize, initial value \( x_0 \).

Output : Lyapunov exponents for each parameter value

1. parameter = parameter start
2. While parameter < parent
   2.1 If \( \left| \frac{dx_{n+1}}{dx_n} (n = i) \right| < 10^{-15} \), Lyapunov Exponent = -inf, end if
      else
      2.1.1 Summage = 0
      2.1.2 for i = 0 to n-1
          summage = summage + \( \ln \left| \frac{dx_{n+1}}{dx_n} (n = i) \right| \)
      2.1.3 summage = summage/n
      2.1.4 Lyapunov Exponent = summage
   2.2 parameter = parameter + stepsize
3. Find the best Lyapunov Exponent and its corresponding parameter
4. End

Figure 1 shows the flowchart of this algorithm.
Next, below is the algorithm for the bifurcation diagram construction, which simply plots the map's values after a sufficiently large numbers of iterations corresponding to the values of the parameters used.

**Algorithm 2.** Bifurcation diagram constructor:

Input: chaos map, parameter start, parend, start (wait time for plot), number of plots per parameter n, stepsize, initial value $x_0$.

Output: Lyapunov Exponents for each parameter value

1. parameter = parameter start
2. While parameter < parend
   1. Calculate $\frac{dx_{n+1}}{dx_n}$
   2. Calculate and plot $x_{start+1}, x_{start+2}, x_{start+3}, ..., x_{start+n}$
   3. parameter = parameter + stepsize
3. End

Figure 2 shows the flowchart of this algorithm.

**Figure 1.** The Lyapunov Exponent Calculation Algorithm

**Figure 2.** The Bifurcation Diagram Construction Algorithm
Finally, we conduct the NIST test using a Python implementation of this test developed by Steven Kho Ang [24]. Below are our steps to subject our maps to the test.

1. Construct the map to be tested (since the general function has already been constructed, this is done by choosing the parameter values).
2. Take an initial value and record all of the map's value for 125000 iterations.
3. Perform a transformation on the values so that they become integers ranging from 0 to 255.
4. Transform all of the integers into 8-bit binary strings.
5. Concatenate all of the 125000 strings sequentially to form a single binary string with 1000000 bits, and input it into the NIST test.
6. The test will decide whether the sequence passes each of the 16 NIST tests, from which, we can conclude whether the map is a good RNG.

3. An Overview of the Gauss and the Circle Map

Before we enter the main analysis of the proposed map, we need to analyze the Gauss Map and the Circle Map to seek its best parameters for the best chaotic properties, as an effort to optimize the newly constructed map. For this purpose, we will plot some bifurcation diagrams and Lyapunov Exponent graphics for both maps, from which we refer to it for further calculations.

3.1 The Gauss Map

The Gauss Map is defined as [20]

\[ x_{n+1} = e^{-\alpha x_n^2} + \beta \]  

where \( \alpha \) and \( \beta \) are real numbers with \( \alpha > 0 \) (otherwise, unbounded and not chaotic). Interesting chaotic properties occurs around \(-1 \leq \beta \leq 1\) on the Gauss Map, where the value of the map asymptotically oscillates around \(-1\) and 1.25. We also have

\[ \frac{dx_{n+1}}{dx_n} = -2\alpha x_n e^{-\alpha x_n^2} \]  

The Gauss Map shows one of its strongest chaotic behavior at \( \alpha = 10 \) and \( \beta = -0.6 \), with a Lyapunov Exponent of 0.6390772819440774. Figure 3 below shows the bifurcation diagram of the Gauss Map and its corresponding Lyapunov Exponent graphic when \( \alpha = 10 \).

![Figure 3. The Gauss Map for \( \alpha = 10 \)](image-url)
3.2 The Circle Map

The Circle Map is defined as [21]

\[
x_{n+1} = (x_n + \Omega + \frac{K}{2\pi} \sin(2\pi x_n)) \mod 1
\]

where \(\mod 1\) denotes the decimal part of a number, or mathematically,

\[
x \mod 1 = x - \lfloor x \rfloor
\]

so that the map value is always lower than 1 but not less than 0, and \(\Omega, K\) are any real numbers, where \(\Omega\) can be limited at \(0 \leq \Omega < 1\), as it is a single addition term in this modulo 1, so all other values of \(\Omega\) have been represented by this interval.

This map exhibits a very interesting property. It has an unlimited chaotic potential. As the value of \(\Omega\) moves away from 0, its Lyapunov Exponent increases continuously, though it may drop at some points, and that the increment slows down. Therefore, we can just choose the value of \(K\) as high or as low (negative) as we want to get a sufficiently high Lyapunov Exponent. Furthermore, the significance of the value of \(\Omega\) towards the behavior of the Circle Map decreases as \(K\) goes further away from 0.

To justify our findings, below are some plots for this map.

\[ -2\pi \leq K \leq 2\pi, \Omega = 0 \]

\[ 999997 \leq K \leq 1000003, \Omega = 0.5 \]

Figure 4. Some Circle Map plots
4. The New Proposed Map and Results

Below is our new proposed map, the improved version of the Gauss Map, named the Gauss-Circle Map, defined as

\[ x_{n+1} = e^{-\alpha\left(\frac{5}{4}\left(x_n + \beta + \frac{K}{\pi} \sin(2\pi x_n)\right) \mod 1\right)^{1/2}} + \beta \]  

(5)

where \(\alpha, \beta, K, \) and \(\Omega\) are real numbers with \(\alpha > 0\). Here, the Gauss Map becomes the main function of the Map, while the Circle Map is composed within. Since the value of the map is expected to be oscillating between \(-0.5\) and \(0.75\), as is the chaotic value range of the Gauss Map, we need to adjust the Circle Map that becomes the “variable” of the original Gauss Map and has a range of the semi-closed interval \([0,1)\) to also have this value of range, so that the original Gauss Map’s chaotic property can be fully utilized. It is simply done by multiplying the Circle Map by \(\frac{5}{4}\) and then subtracting it by \(\frac{1}{2}\), because the closed interval \([-0.5,0.75]\) is \(\frac{5}{4}\) times longer and has a lower bound \(\frac{1}{2}\) lesser than the semi-closed interval \([0,1)\).

Meanwhile, inside the Circle Map itself, no adjustments are required, since if \(\Omega\) is sufficiently large, it is already very chaotic. The derivative of this Map for the Lyapunov Exponent calculation is

\[ \frac{dx_{n+1}}{dx_n} = e^{-\alpha\left(\frac{5}{4}\left(x_n + \beta + \frac{K}{\pi} \sin(2\pi x_n)\right) \mod 1\right)^{1/2}} \cdot \left(1 - \frac{5}{4}\left(x_n + \beta + \frac{K}{\pi} \sin(2\pi x_n)\right) \mod 1\right) \cdot \frac{5}{4} (1 + K \cos(2\pi x_n)) \]  

(6)

Below is a table that compares the best Lyapunov Exponents of the original and the modified Gauss Map within \(-1 \leq \beta \leq 1\). For the modified map, we use \(K = 1000000\) and \(\Omega = 0.5\).

| \(\alpha\) | \(\beta\) (original) | Best Exponent (original) | \(\beta\) (modified) | Best Exponent (modified) |
|-------|-----------------|--------------------------|---------------------|-------------------------|
| 1     | 0.099           | -0.15406087304527474     | -0.432              | 12.878834941293368     |
| 2     | -0.53           | -0.00611141858431256     | -0.86               | 13.322306509793357     |
| 3     | -0.719          | -0.00652064867412348     | -0.878              | 13.55036719284928     |
| 4     | -0.359          | -0.00622587511076678     | 0.165               | 13.63322732459665     |
| 5     | -0.483          | 0.2236351470472602       | -0.427              | 13.67452450360994     |
| 6     | -0.597          | 0.4027270337348413       | 0.53                | 13.700242189243399    |
| 7     | -0.657          | 0.44567601025073833      | 0.49                | 13.688088856757078    |
| 8     | -0.568          | 0.5217138996713785       | 0.456               | 13.71227118853673     |
| 9     | -0.628          | 0.594307609017837       | 0.481               | 13.730089596278177    |
| 10    | -0.6            | 0.6390772819440774       | 0.975               | 13.698301159095992    |
| 11    | -0.53           | 0.591255622709812       | -0.019              | 13.675831473589184    |
| 12    | -0.51           | 0.561588560991265       | -0.014              | 13.65010302273050      |

We limit our observation at \(\alpha = 12\) as the Lyapunov Exponents constantly lowers with the increasing value of \(\alpha\) beyond that value. From Table 1, we can see that some of the best maps for its chaotic behavior is the one with \(\alpha = 10\) and \(\beta = -0.6\) for the original Gauss Map and \(\alpha = 9, \beta = 0.481, K = 1000000,\) and \(\Omega = 0.5\) for the modified Gauss Map, that is, respectively,

\[ x_{n+1} = e^{-10x_n} - 0.6 \text{ and } x_{n+1} = e^{-9\left(\frac{5}{4}\left(x_n + 0.5 + \frac{500000}{\pi} \sin(2\pi x_n)\right) \mod 1\right)^{1/2}} + 0.481 \]  

(7)
Therefore, we conduct the NIST randomness test on both maps as in (7) and compare their results in Table 2. As a note, (O) and (M) is the original and the modified Gauss Map respectively.

Table 2. NIST test comparison between the Gauss Map and the Gauss-Circle Map

| Type of Test                          | P-Value (O)       | Conclusion (O) | P-Value (M)       | Conclusion (M) |
|--------------------------------------|-------------------|----------------|-------------------|----------------|
| 01. Frequency Test (Monobit)         | 0                 | Non-Random     | 1.24×10^{-34}    | Non-Random     |
| 02. Frequency Test within a Block    | 0                 | Non-Random     | 1.09×10^{-258}   | Non-Random     |
| 03. Run Test                         | 0                 | Non-Random     | 0                 | Non-Random     |
| 04. Longest Run of Ones in a Block   | 1.4×10^{-270}     | Non-Random     | 5.03×10^{-141}   | Non-Random     |
| 05. Binary Matrix Rank Test          | 0                 | Non-Random     | 0.246079         | Random         |
| 06. Discrete Fourier Transform (Spectral) Test | 9.23×10^{-14}    | Non-Random     | 3.92×10^{-18}    | Non-Random     |
| 07. Non-Overlapping Template Matching Test | 4.38×10^{-29}   | Non-Random     | 0                | Non-Random     |
| 08. Overlapping Template Matching Test | 1.97×10^{-98}   | Non-Random     | 0                | Non-Random     |
| 09. Maurer's Universal Statistical test | 0                 | Non-Random     | 6.57×10^{-135}   | Non-Random     |
| 10. Linear Complexity Test           | 0.38543           | Random         | 0.556307         | Random         |
| 11. Serial test:                     | 0                 | Non-Random     | 8.37×10^{-5}     | Non-Random     |
| 12. Approximate Entropy Test         | 0                 | Non-Random     | 0                 | Non-Random     |
| 13. Cumulative Sums (Forward) Test   | 0                 | Non-Random     | 3.78×10^{-135}   | Non-Random     |
| 14. Cumulative Sums (Reverse) Test   | 0                 | Non-Random     | 5.09×10^{-135}   | Non-Random     |
| 15. Random Excursions Test           | 0.849145*         | Random         | 0.745552*        | Random         |
| 16. Random Excursions Variant Test   | 0.617075*         | Random         | 0.586214*        | Random         |

Here, we can see that there is not much difference on the test result quality of the new map compared to the original, although most of the P-Values from each test gains improvements. Each test is passed by the maps if its P-Value result is at least 0.1.

For further detail, below is the bifurcation diagram and the Lyapunov Exponents of the Gauss-Circle Map with $\alpha = 9, K = 1000000, \Omega = 0.5$.

The figure above shows how the Lyapunov Exponents ranges between 12 and 14 and how the Gauss-Circle Map asymptotically oscillates between $b$ and $b + 1$, which is reasonable as the exponential part with negative power in equation (5) of the map would vary between 0 and 1,
In chaos based cryptography, the Lyapunov Exponent value of the chaotic map used in a cryptosystem determines how close must the key be chosen to the actual key value used for encryption when performing a brute force cryptoattack, while the bifurcation diagram of the map can be used to observe the uniformity of the number sequence generated by the map to secure the cryptosystem from statistical attacks. Therefore, as shown by the diagrams in Figure 5 and the NIST test results, we conclude that when this Gauss-Circle Map is implemented for cryptography, the cryptosystem will have an excellent sensitivity to initial conditions, yet poor uniformity in map value distribution, giving the encryption result a rather imbalanced histogram and making it rather prone to statistical attacks.

5. Discussion
One of the most important manipulation used here for the new map is the effort to conserve the map value to range within the original Gauss Map asymptotical value range. This causes the Gauss-Circle Map value to oscillate unpredictably as in the original Gauss Map, and is one of the main reason why the chaotic property of the original Gauss Map can be preserved. Another important effort is simply including the strongly chaotic Circle Map in the new map as the "variable" of the modified Gauss Map, causing the new map value to not only experience the Gauss Map's value oscillation, but also the Circle Map's value oscillation, increasing the complexity of the map's dynamics.

The Lyapunov Exponent analysis result shows that the modified Gauss Map has much higher Lyapunov Exponents than the original, meaning that it has much more sensitivity to initial conditions. However, the new map is still not an excellent candidate for a RNG, despite several improvements from the best original Gauss Map's quality. The reason can be seen from its bifurcation diagram in Figure 5, where its density is not uniform, and tend to condense in the upper and lower edge of its asymptotical values limits. For instance, for $\alpha = 9, b = 0.5, K = 1000000$, and $H = 0.5$, the Gauss-Circle Map's value tend to stick near 0.5 and 1.5, meaning that most of the numbers in the sequence generated by this map are very close to those values.

Furthermore, it is reasonable that the chaotic behavior of both Gauss Maps weakens when the value of $\alpha$ becomes too large, because the higher the value of $\alpha$ in the function $f(x) = e^{-ax^2}$, the faster the value of $f(x)$ approaches to 0 as the value of $x$ moves away from 0. This implies that an excessive value of $\alpha$ will shorten the Gauss Map's asymptotical value range.

6. Conclusion
The composition of the Circle Map into the Gauss Map along with an additional modification has successfully generated the Gauss-Circle Map that has a significantly greater sensitivity to initial conditions, although it is still not very suitable for a RNG as it only passes 4 out of 16 NIST test, meaning that its randomness level is only at 25%. Therefore, if this Gauss-Circle Map is utilized for cryptographic purposes, the cryptosystem that utilizes it will have a strong brute force attack resistance, but may be weak against statistical attacks. Further analysis and efforts may be done to improve the map, such as seeking better parameters, performing different or additional manipulations to the new map.

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] Eva N and Suryadi MT, (2013). Chaos-Based Encryption Algorithm for Digital Image *Proceedings IICMA* 169-177

[3] 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

[4] 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

[5] 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

[6] Laptyeva TV, Flach S and Kladko K, (2011). The weak password problem: Chaos, criticality, and encrypted p-CAPTCHAs *EPL* 95 981-981

[7] Shujun L and Xuan Z, (2002). Cryptanalysis of a chaotic image encryption method *International Symposium on Circuits and System* 87-91

[8] Qinan L, (2011). Color image encryption algorithm and its decryption method protecting from shearing attack *Computer engineering and design* 32 509-512

[9] Suryadi MT, Nurpeti E, Widya D, (2014). Performance of Chaos-Based Encryption Algorithm for Digital Image *TELKOMNIKA* 12 675-682

[10] Sun F, Liu S and Li Z, (2008). A novel image encryption scheme based on spatial chaos map *Chaos Solitons Fractals* 38 631-640

[11] 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

[12] 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

[13] Pareek NK, (2012). Design and Analysis of a Novel Digital Image Encryption Scheme *International Journal of Network Security & Its Applications* 4, 95-108

[14] 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.

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

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

[17] 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).

[18] 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*.

[19] 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.
[20] Hemanta Kr. Sarmah, Mridul Chandra Das, Tapan Kr. Baishya and Ranu Paul, (2016). Characterising Chaos In Gaussian Map International Journal of Advanced Scientific and Technical Research 6 160-172

[21] Philip L. Boyland, (1986). Bifurcations of circle maps: Arnol’d tongues, bistability and rotation intervals. (Berlin: Springer-Verlag)

[22] 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 Revision 1a

[23] Stephen Lynch, (2010). Dynamical Systems with Applications using Maple Second Edition, (Boston: Birkhäuser)

[24] Python implementation of NIST's A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
https://github.com/stevenang/randomness_testsuite