BAREKENG: Journal of Mathematics and Its Applications
September 2023 Volume 17 Issue 3 Page 1553–1564
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol17iss3pp1553-1564

ANALYSIS OF NEW CHAOTIC MAP AND PERFORMANCE EVALUATION IN ITS APPLICATION TO DIGITAL COLOR IMAGE ENCRYPTION

Ita Mar'atu Solihat [1*], **Suryadi MT** [2], **Yudi Satria** [3]

[1,2,3]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia*
Depok, 16424, Indonesia

*Corresponding author's e-mail: ** ***ita.maratu@sci.ui.ac.id***

ABSTRACT

Article History:

Received: 17th March 2023
Revised: 6th August 2023
Accepted: 15th August 2023

Keywords:

New Chaotic Map;
Bifurcation diagram;
Lyapunov exponent;
Encryption;
Decryption.

In this research, a new chaotic map, which is a modification from the composition of the MS map and an Improved logistics map, is proposed. The new map's chaotic behavior is proven by the bifurcation diagram and Lyapunov exponent. This map will be used in chaos-based cryptography as a keystream generator, and then it will be processed in the encryption and decryption algorithms through XOR operations. The results of the encryption and decryption processes were evaluated by several tests, such as key sensitivity analysis, histogram analysis, correlation analysis, and image quality analysis. All the tests are done to evaluate the performance of the new chaotic map in the encryption of digital color images. Based on the results of several tests, a conclusion can be drawn that the encryption and decryption process is successful and difficult to attack with various kinds of attacks. The key that is built from a new chaotic map has a good sensitivity.

How to cite this article:

I. M. Solihat, Suryadi MT and Y. Satria., "ANALYSIS OF NEW CHAOTIC MAP AND PERFORMANCE EVALUATION IN ITS APPLICATION TO DIGITAL COLOR IMAGE ENCRYPTION," *BAREKENG: J. Math. & App.*, vol. 17, iss. 3, pp. 1553-1564, September, 2023.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article • Open Access

1. INTRODUCTION

Advances in information, communication technology, and multimedia have made a big impact in this era. The transmission of information from various types of digital data both text, images, and videos run so massively with its convenience. A lot of data that is very sensitive distributed or stored digitally. Without proper security, data will be highly vulnerable to “attacks” such as unauthorized deletion, modification, copying or addition during transmission or while data is stored. In order to have good security, information must be hidden from unauthorized access or *confidential*, protected from unauthorized change or have *integrity*, and can be accessed by authorized entities when information is needed or *availability* [1]. To protect transmitted and stored data, there are several ways that can be done, namely by watermarking, encryption, and steganography [2]–[7]. From that three methods, encryption is one of the important methods and is very suitable and also efficient in preventing attacks [4].

In science, the existence of chaos theory has become a hot topic for researchers. Typical behaviors of chaos that are interesting to study are *unpredictability*, *ergodicity*, *pseudo-randomness*, and *high sensitivity to initial value conditions* [1], [3], [8]–[11]. Because of this distinctive behavior, many scientists have researched the benefits of chaos including observing the relationship between characteristics of chaos and cryptography. One example of its application is chaos theory-based image encryption. Chaos theory is applied in the form of map that has the typical behavior of chaos and is called chaotic map. Furthermore, the chaotic map is used as a *keystream* generator of a cryptosystem. In general, chaotic maps are divided into two types, namely one-dimensional chaotic maps (1D) and multidimensional chaotic maps (MD). The difference between 1D and MD are the structure and complexity of computation. MD chaotic maps have high structure and computational complexity and 1D in terms of structure is very simple and has low computational complexity. Although MD theoretically exhibits superior chaotic properties, *1D* chaotic map are more often used due to their simplicity. Even so, the simplicity of 1D is followed by several problems including limited chaotic range, non-uniform distribution, and limited scope of application [3], [12]–[14]. In cryptography, these problems cause encrypted data to be easily penetrated by various attacks. Therefore, researchers tried to overcome these problems including by modifying the shape of the chaotic map as done by Maria [15], making a general equation where if included by the 1D chaotic map then the chaotic range changes to be wider [13], composing two chaotic maps [7], [8], [16], [17].

Based on this explanation, in this research of a new chaotic function will be created where prospect will be used as a *keystream* generator. The method used to obtain this chaotic function is by composing two 1D chaotic functions, namely *Improved logistic map* made by Pak *et al*. [13] and MS *map* made by Maria [15] then the results are modified into a simpler form. The uniqueness of this new function is derived from two functions where both are improvisations or modifications of the *Logistic map* but have better performance in digital data encryption. In addition, research on the composition of two chaotic functions that were later modified is still limited and there has been no research that has carried out compositions from the results of modifications or improvisations of the same chaotic map such as MS *map* and *Improved logistic map*. The results of this research are expected that the new chaotic map can minimize the shortcomings of the *Logistic map* so that it will become more difficult to decrypt illegally.

2. RESEARCH METHODS

2.1 Construction of a new *chaotic map*

Known general forms of MS *map* and *Improved logistic map* are as follows:

MS *map* [15]:

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

With

Improved Logistic Map [13]:

$$x_{n+1} = mod\big(\big(u\,x_n\,(1-\ x_n) - (4-u)x_n\,(1-\ x_n\,)\big)\ \times\ 2^{12}, 1\big) \tag{2}$$

If $f(x_n)$: MS *map* and g(x$_n$) : *Improved logistic map*, hence the composition of $f(x_n)$ and $g(x_n)$ is

$$x_{n+1} = \frac{r\lambda((2x_n(u(1-x_n)+2(x_n-1)))2^{12}(mod\ 1))}{1+\lambda(1-(2x_n(u(1-x_n)+2(x_n-1))\ 2^{12}(mod\ 1)))^2}\ (\text{mod } 1) \qquad (3)$$

After the composition function is formed, the modification process is carried out to form a function that is simpler than the composition function. Symbol λ is a symbol to express the magnitude of *Lyapunov exponent* so the first change is made by changing the symbol λ in **Equation (3)** into p so there is no confusion or double definition of symbol λ. Modification is done by eliminating the operation $modulo$ 1 on numerators and denominators due to the use of $modulo$ 1 is used to ensure the domain and codomain are in *the same range*, namely:$(0-1)$. Further modification was made by $trial\ and\ error$ technique against 2^{12} which is based on the assumption that the equation will be simpler and can save *keystream* formation time. Based on this, an experiment was conducted with the system performing the calculation process on fractions first and then a multiplication operation with 2^{12}. Here is the results of the second modification:

$$x_{n+1} = \left(\left(\frac{rp(2x_n(u(1-x_n)+2(x_n-1)))}{1+p(1-2x_n(u(1-x_n)+2(x_n-1))^2}\right) \times 2^{12} \right) mod1 \qquad (4)$$

where:

r is in range [0.1 – 4]

p is in range [0.1 – 4]

u is in range $[0-1.9]\ \cup\ [2.1-4]$

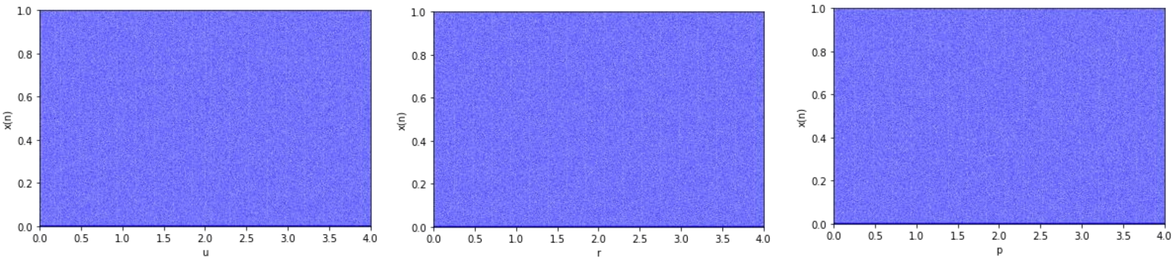
x is between [0 – 1]

2.2 Analysis of New *Chaotic Map*

The first step after the new map is formed is to analyze whether the map has chaotic properties or not by analyzing the *bifurcation diagram* and *Lyapunov exponent* of the map. A bifurcation diagram is a diagram that shows asymptotic points as a function of parameter values **[18]**. Bifurcation diagram illustrates the possible long-term changes of system behavior when the values of control parameters are varied so that they can be analyzed by varying one parameter at a time. In a bifurcation diagram, stable values are represented by lines and for unstable values are represented by dots. In the new *chaotic map*, there are three parameters, namely parameters u, p and r. Each parameter will be seen as what the bifurcation diagram looks like when the values of the other two parameters are varied. To prove that a map *sensitive dependence* on the initial value can be seen using *Lyapunov exponent*. *Lyapunov exponent* is very useful in looking at the characteristics of chaos in a system because it is a quantity that states *the* speed of separation of two trajectories that are very close together over time. Lynch **[18]** said that a map issaid to be *chaotic* if there is at least one positive *Lyapunov exponent*. *Lyapunov exponent* for a map $x_{n+1} = f(x_n)$ is a function of the intial value x_0, denoted by λ. Here is the forula to calculate the *Lyapunov exponent* **[19]**:

$$\lambda = lim_{n\to\infty} \left\{ \frac{1}{n} \sum_{i=0}^{n-1} ln|f'(x_i)| \right\} \qquad (5)$$

Based on the analysis conducted on the bifurcation diagram and *Lyapunov exponent*, this time the study was conducted experiments on each parameter with values $x_0 = 0.6$ as well as parameters $r = 3.15,\ p = 2$, and $u = 3.9$. The following is the bifurcation diagram of each parameter.

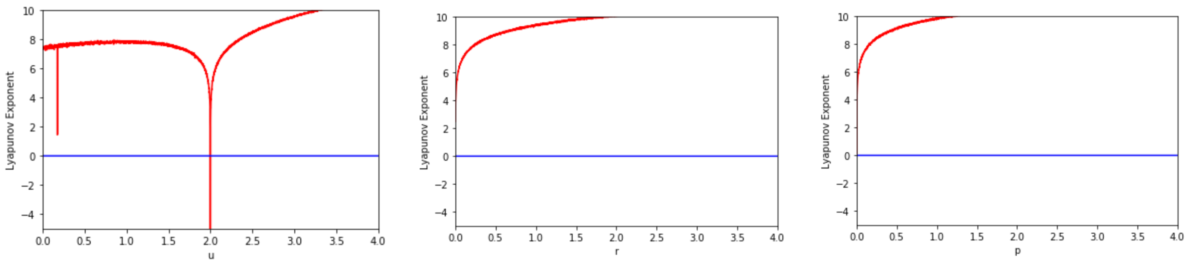


(a) **(b)** **(c)**

Figure 1. (a) Bifurcation diagram with $r = 3.15$ and $p = 2$, (b) Bifurcation diagram with $u = 3.9$ and $p = 2$, (c) Bifurcation diagram with $r = 3.15$ and $u = 3.9$

In **Figure 1**, all bifurcation diagrams show that in the range $[0-4]$, each parameter shows *chaotic* behavior. This is indicated by dense periodic points in the *range*.

The Lyapunov exponent calculation serves to see that the map is sensitive to the initial value. Here is a sample image of the *Lyapunov exponent* from the new chaotic map.



(a) (b) (c)

Figure 2. **(a)** ***Lyapunov exponent*** **with** $\boldsymbol{r = 3.15}$ **and** $\boldsymbol{p = 2}$**, (b)** ***Lyapunov exponent*** **with** $\boldsymbol{u = 3.9}$ **and** $\boldsymbol{p = 2}$**, (c)** ***Lyapunov exponent*** **with** $\boldsymbol{r = 3.15}$ **and** $\boldsymbol{u = 3.9}$

Based on **Figure 2**, it can be seen that the *Lyapunov exponent* for each parameter is positive, this indicates that two adjacent trajectories are moving divergently. A positive value from this calculation indicates that the new chaotic map is sensitive to the initial value.

The bifurcation and *Lyapunov exponent* diagrams listed in **Figure 1** dan **Figure 2** all use the values of $x_0 = 0.6$ and parameters $r = 3.15$, $p = 2$ dan $u = 3.9$. From the results of the bifurcation diagram and *Lyapunov exponent*, it can be concluded that the selection of initial values and parameters in this study is fairly good because all of them have *chaotic* properties. Therefore, these values will then be used in generating the *keystream* array.

After getting the conclusion that the new map formed is chaotic, the encryption and decryption process is carried out based on the new chaotic map. The following is the *pseudocode* of the *keystream* generation algorithm, encryption algorithm, and decryption algorithm.

Algorithm 1. *Keystream* Generator Algorithm

```
Input : $x_0$, $u$,$p$ and $r$
Output : keystream
Read  $x_0$, parameters value, data size (n)
For i = 1: (n) do
    y = new chaotic map ($r, p, u, x$)
    sequence[i] = y
    x = y
end for
csequence = round(sequence*100000) mod 256
stop
```

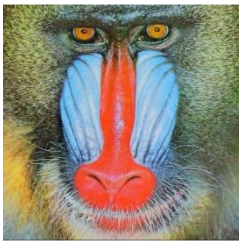
Algorithm 2. Encryption Algorithm

```
Input : original image
define a zero matrix datac the size of data (original image)
l = 0
for i = 0: m-1 do
   for j = 0: n-1 do
      for k = 0:3 do
         datac[i,j,k] = data[i,j,k]⊕csequence[l]
          l = l + 1
      end
   end
end
Output : Encrypted image
```

2.3 Data Image

There are four color images data with varying sizes that will be used for testing in this study. The following is a table that displays test data in detail:

Table 1. Detail Image Data

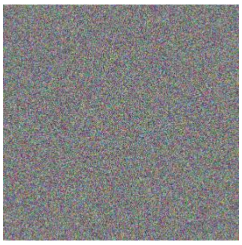
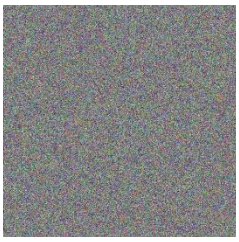
Image Name	Original Image	Dimensions (Pixel)	Source
Baboon		512×512	https://github.com/scijs/baboon-image
vegetable		425×282	https://knowledgedo.in/10-lines-on-fruits-and-vegetables/
lenna		512×512	https://en.wikipedia.org/wiki/Lenna#/media/File:Lenna_(test_image).png
fish		1920×1200	https://www.wallpaperflare.com/water-sea-animals-fish-underwater-1920x1200-animals-fish-hd-art-wallpaper-btcfs

3. RESULTS AND DISCUSSION

3.1 Encryption and Decryption Trial Results

In this trial, researchers used key parameters $x_0 = 0.6$, $r = 3.15$, $u = 3.9$, and $p = 2$. The results of the test in Table 2. show that the appearance of encrypted image is very different from the original image and it is unpredictable what the original image looked like before being encrypted. In addition, the decrypted image has the same appearance as the original image to the naked eye. Based on these results, it can be said that the encryption and decryption algorithm are successful. And for the new chaotic map as a *keystream* generator has good quality.

Table 2. Display of Image Data Encryption and Decryption Trial Results

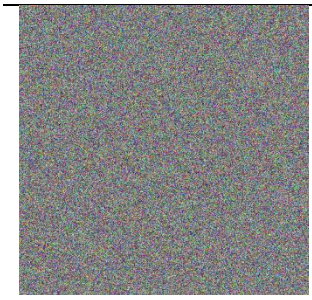
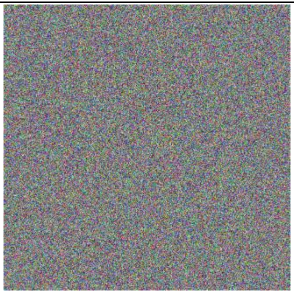
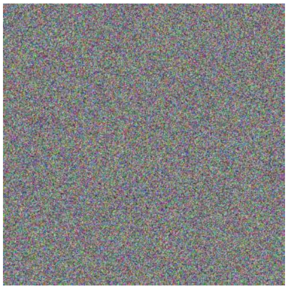
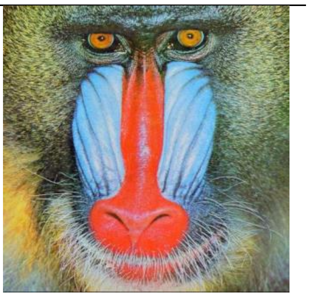
Image Name	Original Image	Encrypted Image	Decrypted Image
Baboon			
vegetable			
lenna			
fish			

3.2 Analysis of Trial Results

Key Sensitivity Analysis

A cryptosystem must be very sensitive if there is a very small change, in other words, *chiperimage* cannot be decrypted, even if there is very little difference between encryption key and decryption key. To find out how sensitive the key of the new *chaotic map* is, changes will be made to the value of the existing parameters with a very small difference in value from the key that should be in the decryption process. In the first test, a change in value r each $3.15 + 10^{-5}, 3.15 + 10^{-10}, 3.15 + 10^{-13}$, and $3.15 + 10^{-14}$. Furthermore, the test is carried out by changing the value of p with their respective changes $2 + 10^{-5}, 2 + 10^{-10}$, $2 + 10^{-15}$, and $2 + 10^{-16}$. For value change u which is $3.9 + 10^{-5}$, $3.9 + 10^{-10}$, $3.9 + 10^{-14}$, and $3.9 + 10^{-15}$.

Table 3. Sensitivity Test Results for Value Changes r

$r = 3.15 + 10^{-5}$	$r = 3.15 + 10^{-10}$	$r = 3.15 + 10^{-13}$	$r = 3.15 + 10^{-14}$
			

According to Table 3 the difference in parameter values r entered in the decryption process of 10^{-5}, 10^{-10}, and 10^{-13} does not successfully show the original image. When the parameter value is 3.15000000000001 or $3.15 + 10^{-14}$, the original image is recognized and the decryption process is successful.

Table 4. Sensitivity Test Results for Value Changes u

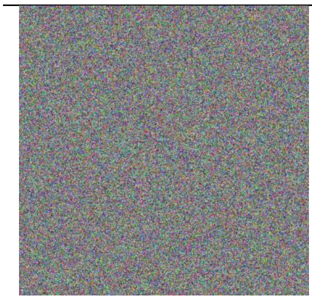
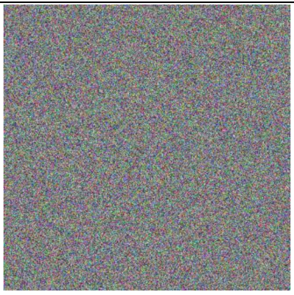
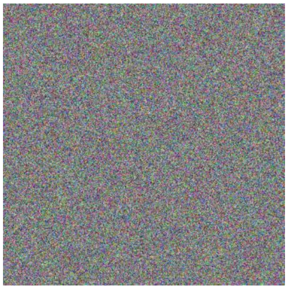
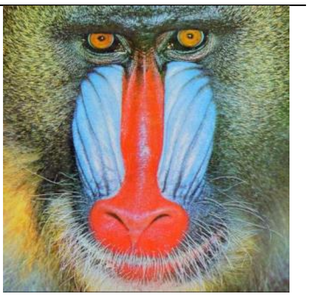
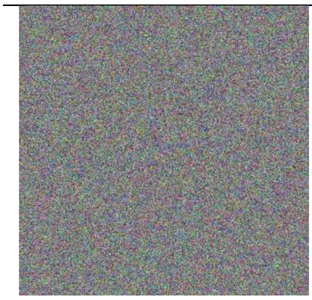
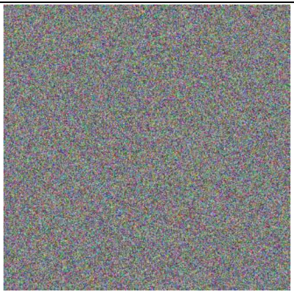
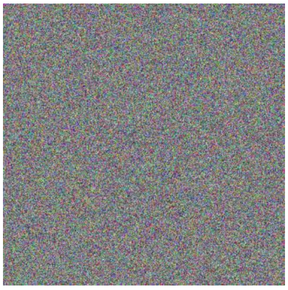
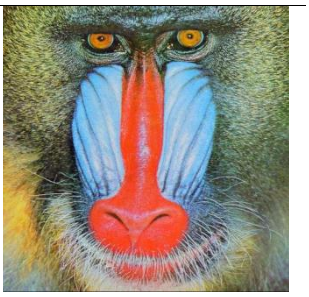
$u = 3.9\ + 10^{-5}$	$u = 3.9 + 10^{-10}$	$u = 3.9 + 10^{-14}$	$u = 3.9 + 10^{-15}$
			

Table 4 shows the results that when the value of parameter u entered in the decryption process is $3.9\ + 10^{-5}$, $3.9\ + 10^{-10}$, and $3.9\ + 10^{-14}$ is unable to show the original image, but when the value entered is $3.9\ + 10^{-15}$ the result of the decryption process shows the original image. This shows that with the difference of 10^{-14} from the actual value of parameter u, the original image still cannot be identified because the system considers that the key entered is wrong.

Table 5. Sensitivity Test Results for Value Changes p

$p = 2 + 10^{-5}$	$p = 2 + 10^{-10}$	$p = 2 + 10^{-15}$	$p = 2 + 10^{-16}$
			

The results of the sensitivity test for changes in parameter p as shown in Table 5 can be concluded that the difference in values as large as 10^{-5}, 10^{-10} and 10^{-15} from the initial value of p which is 2 in the decryption process is not able to show the original image. The results of the decryption process began to show the original image when the value entered was $2 + 10^{-16}$ or had a difference of 10^{-16}.

Based on the test results of Table 3, Table 4, and Table 5, it is concluded that the parameter sensitivity p is equal to x_0 which is 10^{-15} while the parameter r and u each show a sensitivity of 10^{-13} and 10^{-14} .

With a value of 10^{-15}, 10^{-13} and 10^{-14} for key sensitivity values are fairly good or very sensitive so that the cryptosystem can withstand *brute force attacks*.

The next step is to calculate the sensitivity level by calculating the *Number of Pixel Changing Rate* (NPCR) and *Unified Average Changing Intensity* (UACI). NPCR and UACI are each used to calculate the percentage of pixel differences in two encrypted images with keys whose differences are very small and test the difference in the average intensity values of the two encrypted images. Here is the formula for calculating NPCR and UACI [1].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (6)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{I,J} \frac{C_1(\mathrm{i,j}) - C_2(\mathrm{i,j})}{255}\right] \times 100\% \qquad (7)$$

The optimal values for NPCR and UACI are 99.61% and 33.46%, respectively [20].

Table 6. NPCR and UACI Test Result

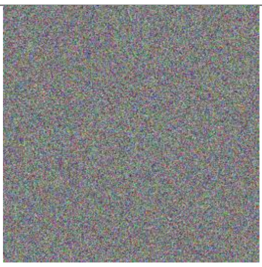
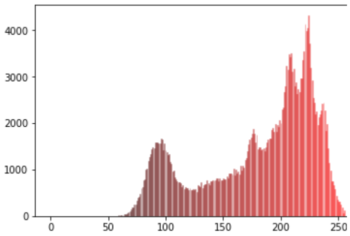
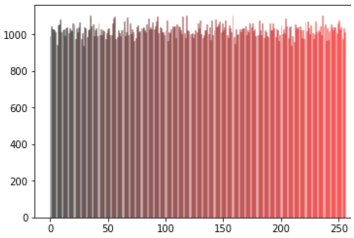
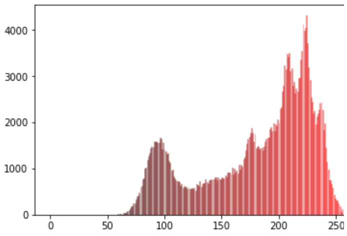
Image Name	NPCR	UACI
Baboon	99.62514241536458	33.498011570361115
Vegetable	99.60061187595606	33.35531178680265
Lenna	99.61624145507812	33.35346745510837
Fish	99.62335069444445	33.381551776769534

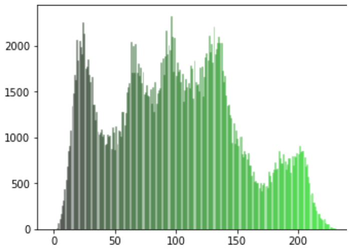
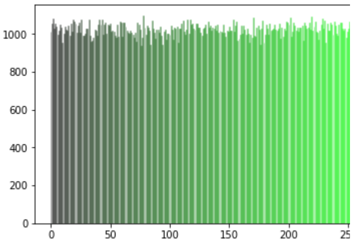
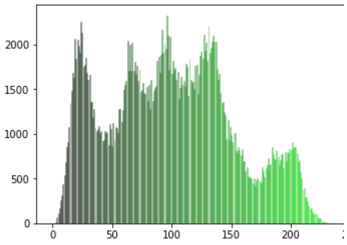
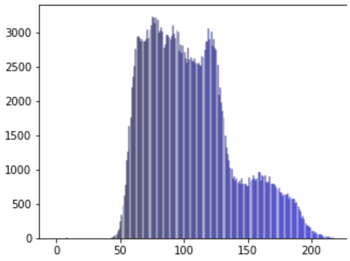
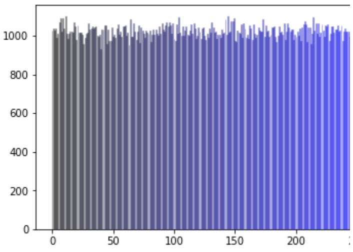
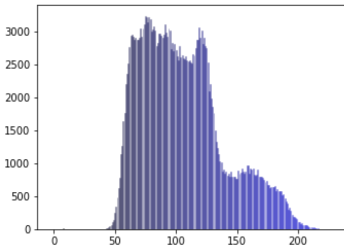
Based on Table 6, the new chaotic map has NPCR and UACI values on each tested data around the optimal values of 99.61% and 33.46%. This shows that the proposed new chaotic map has good key sensitivity as has been proven by value shift test.

Histogram Analysis

In digital image analysis, a histogram is one way to show what the color distribution looks like in an image. In an encrypted image, the histogram diagram will look flat or *uniform*, in other words, the color distribution is uniformly. In color images, the histogram diagram will be divided into three types, they are *red*, *green*, and *blue* component. Table 7 shows the histograms of Lenna image samples in the form of original image, encrypted image, and decrypted image histograms.

Table 7. Histogram of Digital Image

Color Component	Original Image	Encrypted Image	Decrypted Image
			
R			

Color Component	Original Image	Encrypted Image	Decrypted Image
G			
B			

Based on **Table 7**, in the original image, the color distribution in each component is distributed differently according to the number of colors or color intensity, while in encrypted image, the color distribution is equally distributed so that the histogram display is flat. Another case with decrypted image that has histogram display is similar to the original image, so based on the histogram analysis it can be concluded that the decrypted image has the same result as the original image and to make sure the quality of decrypted image same as original image will be known in image quality analysis. To further strengthen that encrypted image is equally or *uniformly* distributed, *a goodness of fit* test is conducted. Here are the results of statistical tests on encrypted images.

Table 8. Statistical Test Results of The New Chaotic Map

Image Name	Statistical Value		
	R Test	G Test	B Test
Vegetable	277.8451397580309	262.9913725490196	255.39147267417604
Lenna	258.29296875	252.884765625	239.8125
Baboon	284.7734375	311.91015625	234.251953125
Fish	252.182	293.34222222222223	230.16311111111111

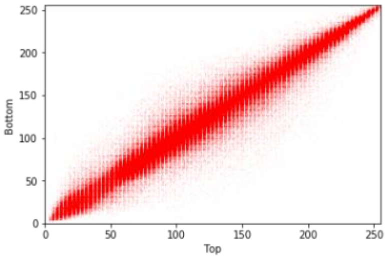
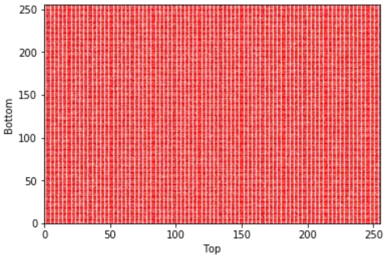
To test whether the resulting statistical value shows the encrypted image is *uniformly* distributed or not, the critical value is determined first. With a free degree of 255 and *a significance level* of 0.01, the critical value for this test is 310.4573882199. For an encrypted image to be *uniformly* distributed, the statistical test value must be less than the critical value. Based on **Table 8**, there is only one value in the Baboon image that exceeds the critical value that is in the G test with 311.91015625. Therefore, it can be concluded that encrypted images are *uniformly* distributed so that statistical attacks cannot be carried out because pixel values are evenly distributed and unpredictable.

Correlation Analysis

The original image has a very high correlation between adjacent pixels, a good encryption algorithm can reduce that correlation so that the encrypted image can withstand statistical attacks. Broadly speaking, between encrypted image and original image should be very different. Correlation analysis is used to calculate how much correlation between pixels in an image. To determine the correlation between two adjacent pixels, this research uses two test methods, there are *scatter plot* and calculation. In both test, five different directions are shown, namely horizontal direction (left-right), vertical direction (up-down), *NW-SE* (North West - South

East, top left - bottom right), NE-SW (*North East* - *South West*, top right - bottom left). The following is the *scatter plot* result of Lenna's image for the new *chaotic map* vertical direction.

Table 9. Scatter Plot Digital Image Correlation

Image Name	Original Image	Encrypted Image
Lenna		

In the original image, the correlation between two adjacent pixels is very strong and the dots converge on the *original* line. While in encrypted image all the points are spread on the *axis* x and y, in other words, there is no correlation between two adjacent pixels. To strengthen the results of *scatter plot correlation* above, the value of the *new chaotic map* correlation calculation will be presented below.

Table 10. New Chaotic Map Correlation Calculation Results

Image Name	Original Image				Encrypted Image			
	Ver	Hor	NW-SE	NE-SW	Ver	Hor	NW-SE	NE-SW
Vegetable	0.9622869443508719	0.9667885798520882	0.93909668286406	0.9425868980948775	-0.000131486054378302	-0.003040156615643382	-0.0020768259346824443	-0.0005243920875978
Lenna	0.9881287699641909	0.9795780555446493	0.97201113706174	0.9773034785277107	-0.000975706614310791	-0.000981642969047316	-0.000460239216509983	-0.0007474101444274659
Baboon	0.8620379474993045	0.9255132614471103	0.83701114022089	0.8315659110845933	-0.001434635211524203	-0.001991570524154699	-0.0006543772139372676	-0.000539882510223422
Fish	0.993775808165202	0.9947511485954275	0.99204190441137	0.9913437280895656	-0.00020130337505915456	-0.002452467630482111	-0.00024056585576805685	-0.000357021021177546

In *plaintext* images or original images, the size of correlation coefficient in each direction both vertically, horizontally and diagonal is always close to one, while in encrypted image that falls into the good category, the size of correlation coefficient is always close to zero. If this happens, it is certain that there will be no correlation between the original image and the encrypted image so that the encrypted image is safe from *statistical* attacks. Table 10 shows that in the original image, all correlation values from all directions close to numbers 1 while in encrypted image, all correlation values are close to zero. The results on the encrypted image show that there is no correlation between two adjacent pixels. Therefore, it can be concluded that the new chaotic map is safe from statistical attacks because the information provided by the encrypted image is not enough to guess the original image.

Image Quality Analysis

In cryptosystems, the decrypted image must be the same as the original image. Therefore, to test the quality of decrypted images in this research using PSNR and MSE tests. *Peak Signal-to-Noise Ratio* (PSNR) is one way that can be used to compare image quality between decrypted images and the original image [15]. When we calculate PSNR we also need the *Mean Square Error* (MSE) value. The following are the results of calculating PSNR and MSE test data using the new *chaotic map*.

Table 11. PSNR and MSE values of the new chaotic map

Image Name	MSE	PSNR
Vegetable	0	∞
Lenna	0	∞
Baboon	0	∞
Fish	0	∞

Based on the table of PSNR and MSE values, new chaotic map is obtained that for MSE are zero, and PSNR are valued ∞ for all images. The results show that the decrypted image is the same as the original image and also has the same quality.

4. CONCLUSIONS

The new chaotic map that formed as a result of modification from the composition of the MS map and *Improved Logistic map* has *chaotic* behavior that can be seen from the *positive Lyapunov exponent and* density on the bifurcation diagram. The implementation of the new *chaotic map-based* image encryption algorithm produces an encrypted image cannot provide any information from the original image because the original image didn't appear and also based on histogram analysis the colour distribution of encrypted image is uniformly distributed. As for the decrypted image, it has the same appearance as the original image and histogram of decrypted image have same distribution as original image. Key sensitivity x_0 and p that is 10^{-15} while the parameters r be 10^{-13} and u be 10^{-14}. In addition, NPCR and UACI values each have values close to the optimal value 99.61% and 33.46%. Based on the results of histogram analysis, the encrypted image on the *chaotic map* is only one point above the critical point value. For correlation analysis, the new *chaotic map* test shows no correlation between two adjacent pixels so that the system is safe from statistical attacks. PSNR and MSE tests performed showed results of 0 and ∞. So it can be concluded that the decrypted image has the same appearance and quality as the original image.

In this study the image used is only a type of color image, so in the next study it can be added by using *greyscale* image. In addition, further modifications of this new chaotic map can be made to produce a better *chaotic map*.

REFERENCES

[1] Ljupco Kocarev and S. Lian, *Chaos-based Cryptography*. Heidelberg: Springer Berlin, 2016.

[2] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[3] X. Wang, Y. Li, and J. Jin, "A new one-dimensional chaotic system with applications in image encryption," *Chaos Solitons Fractals*, vol. 139, p. 110102, Oct. 2020.

[4] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimed. Tools Appl.*, vol. 75, no. 17, pp. 10631–10648, Sep. 2016.

[5] Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, "Effective reversible data hiding in encrypted image with adaptive encoding strategy," *Inf. Sci.*, vol. 494, pp. 21–36, Aug. 2019.

[6] C. Das, S. Panigrahi, V. K.Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *AEU - Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, Mar. 2014.

[7] Ali Mansouri and Xingyuan Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Inf. Sci.*, vol. 520, pp. 46–62, May 2020.

[8] 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*, pp. 210–214, Jun. 2012.

[9] X. Zhou and H. Zhang, "A new chaotic function and its cryptographic usage," *Wuhan Univ. J. Nat. Sci.*, vol. 13, no. 5, p. 557, Nov. 2008.

[10] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.

[11] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, vol. 133, no. 1, pp. 1–14, Jan. 2018.

[12] L. Liu and S. Miao, "An image encryption algorithm based on Baker map with varying parameter," *Multimed. Tools Appl.*, vol. 76, no. 15, pp. 16511–16527, Aug. 2017.

[13] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019.

[14] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimed. Tools Appl.*, vol. 71, no. 3, pp. 1469–1497, Aug. 2014.

[15] M. Y.T. Irsan, "Analsis kinerja new modified map pada enkripsi citra digital," Thesis, Universitaas Indonesia, Depok.

[16] A. Akhsani, H. Mahmodi, and A. Akhvan, "A Novel Block Cipher Based on Hierarchy of One-Dimensional Composition Chaotic Maps," in *2006 International Conference on Image Processing*, pp. 1993–1996 ,Oct. 2006.

[17] S. B. Kembaren, S. Suryadi, and T. Triswanto, "Implementasi algoritma enkripsi citra digital berbasis chaos menggunakan fungsi komposisi logistic dan gauss iterated map," in *Seminar Nasional Pendidikan Sains dan Teknologi*, pp. 263–272 Oktober 2018.

[18] Stephen Lynch, *Dynamical Systems with Applications using Maple^{TM}*, 2nd ed., . 2nd ed., MA: Birkhäuser Boston, 2009.

[19] S. H. Strogatz, *Nonlinear Dynamics and Chaos | With Applications to Physics, Biology*, Second. Second.Boca Raton: CRC Press, 2015.

[20] Y. Wu, J.P. Noonan, and S. Agaian, “NPCR and UACI randomness tests for image encryption,” *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun. JSAT*, vol. 1, no. 2, pp. 31–38, Apr. 2011.