Development of a New Chaotic Function-based Algorithm for Encrypting Digital Images

Dhian Sweetania[1], Suryadi MT[2], Sarifuddin Madenda[3]
Gunadarma University, Department of Information Technology, Depok, 16424, Indonesia[1, 3]
Universitas Indonesia, Department of Mathematics, Depok, 16424, Indonesia[2]

***Abstract*—This paper discusses the development of a new chaotic function (proposed chaotic map) as a keystream generator to be used to encrypt and decrypt the image. The proposed chaotic function is obtained through the composition process of two chaotic functions MS map and Tent map, with the aim of increasing data resistances to attacks. The randomness properties of the keystream generated by this function have been tested using Bifurcation diagrams, Lyapunov exponent, and NIST randomness analysis. All the analysis results indicate that the keystream passed the randomness tests and safe to be used for image encryption. The performance of the proposed chaotic function was measured by way of analysis of its initial value sensitivity, key space, and correlation coefficient of the encrypted image. This function can further increase the resilience against brute force attacks, minimizing the possibility of brute attacks, and has key combinations or key space of 1.05×10^{959} that is much greater than the key space generated by MS Map + Tent Map of 5.832×10^{958}. Finaly, quantitative measurements of encrypted image quality show an MSE value of 0 and a PSNR value of ∞. These values mean that the encrypted image data is the same as its original and both are also visually identical.**

***Keywords*—Chaotic function; decryption; encryption; function composition; key space; MS tent map**

I. Introduction

It is always easy for internet users to obtain various data and information from anywhere and at any time. The development of information technology in the form of text, images, audio and video (multimedia data) and communication is very rapid. Therefore, information security is an absolute matter that must be seriously considered by all users concerned. Information is a very valuable asset for an organization because it serves a strategic resource in increasing value. The information security here concerns policies, procedures, processes and activities to protect information from various types of threats against it that can cause harm to the survival of the organization. Based on this purpose, cryptography is implemented related to information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

In general, cryptography is divided into two parts, namely classical and modern cryptography. Modern cryptography is the development of algorithms from classical cryptography which prioritizes bit mode operations, in contrast to classical cryptography which operates on characters. In one study, there was an encryption system which combined Logistic Map and Henon Map to produce an average PSNR value of less than 10 dB which indicated that the encrypted image had very high noise and an MSE value of more than 400, this means that there are still many signal errors from the original image and cipher image. The length of the process required carrying out the encryption and decryption process was greatly influenced by the size of the dimensions and the number of pixels in a digital image. The encryption system using a combination of Logistic Map and Henon Map took more than 15 seconds to encrypt images that had dimensions of 512×512; however image encryption results were not influenced by the dimensions of the encrypted image [1].

The chaos function has been developed for data encryption in the last decade because of its nature described in [2]. The nature of the chaos function, which is sensitive to the initial conditions, results in a significant difference in the image encryption results. Some of the chaotic functions used in image encryption are Logistic Maps and MS maps. The Logistic Map function has a key space of 10^{30} [3-4], the MS Map function has a key space of up to 3.24×10^{634}[5].

There is an algorithm technique that composes a sequential Logistic Map and Chebyshev Map [6], both of which are used to encrypt medical images. In the initial stage, the medical image is encrypted with a Logistics Map, then an encrypted image is formed, and the image is re-encrypted with a Chebyshev map. Besides that, there is also the Gauss-Circle Map algorithm which is a combination of Gauss Map and Circle Map by combining the two [7] by applying a composition function [8], then proposed a new image encryption algorithm by jointly exploiting overlapping random block partitioning, scanning, double spiral, Henon's chaotic map, and L ü' s chaotic map. Another study proposed a cryptosystem based on 4D Lorenz-type hyper-chaos and deoxyribonucleic acid (DNA) [9].

The MS Map and Tent Map algorithms are two well-known chaotic function algorithms that exhibit chaotic properties, which both have a high potential to generate random keys. Therefore, this paper proposes a new chaotic function which is a composition of the two chaotic functions of MS Map and Tent Map. The proposed function is also chaotic, so it can be used as a random number generator function. This chaotic system is useful for generating random numbers for chaos that has no period. This random number generator is created by compiling a Bifurcation Diagram, Lyapunov Exponent, and the NIST Randomness Test. The chaos system is used as the basis for secure cryptographic algorithms for communication because of the very close relationship between chaos and cryptography [10].

After generating random numbers by composing the MS Map and Tent Map functions, the algorithm performance analysis was carried out based on initial value sensitivity level analysis, key space size analysis, correlation coefficient analysis, and image quality testing (PSNR).

II. RESEARCH METHOD

Two chaotic functions that are often used for data encryption and decryption are MS Map and Tent Map. Both will be used to build a new chaotic function. MS Map is a modification of the Logistic map function as shown by Eq. (1), where $(x\ mod\ 1) = x - \lfloor x \rfloor$ according to the definition. This equation can be expressed recursively as shown in Eq. (2), with initial value $x_0 \in (0, 1)$ and $n = 1,2,3, \ldots$ [5].

$$f(x) = \left(\frac{r\lambda x}{1+\lambda(1-x)^2}\right)(mod\ 1) \quad (1)$$

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

The modulo operation is applied as a congruent function. In a set of integers, congruence is a method or way of explaining the divisibility of an integer. Modulo arithmetic is used in cryptography because the modulo b arithmetic value is in a finite rounded set, namely 0 to $b - 1$. Calculations in the cryptographic process are not outside the set of integers, meaning that the decryption process will not produce a value that is different from the value of the original message. Thus, there is no need to worry about losing information because the rounding occurs as in real number operations.

In mathematics, the Tent map is an iteration chaotic function, which forms a dynamic system based on discrete time. It takes x_n points on a real line and then maps those points to other points [11]. This function can be expressed as in Eq. (3).

$$x_{n+1} = g(x) = \begin{cases} \mu x_n & for\ x_n < ½ \\ \mu(1 - x_n) & for\ x_n \geq ½ \end{cases} \quad (3)$$

Now suppose g is a function from set *A* to set *B* and *f* is a function from set *B* to set *C*. The composition between two functions *f* and *g*, denoted by $(f \circ g)$, is a function from *A* to *C* which is defined as $(f \circ g)(a) = f(g(a))$. Furthermore, if f represents the MS map function in Eq. (2) and g acts as the Tent map function in Eq. (3), so the proposed new chaotic function resulting from the composition of both is expressed in two domain partitions as shown in Eq. (4) and Eq. (5).

$$(f \circ g)(x) = \mu\left(\left(\frac{r\lambda x}{1+\lambda(1-x)^2}\right)(mod\ 1)\right)\ for\ x < ½ \quad (4)$$

Map function was generated from the composition of

$$(f \circ g)(x) = \mu\left(1 - \left(\frac{r\lambda x}{1+\lambda(1-x)^2}\right)(mod\ 1)\right) for\ x \geq ½ \quad (5)$$

Thus, based on Eq. (4) and Eq. (5), the proposed chaotic function can be expressed as in Eq. (6).

$$(f \circ g)(x) = \begin{cases} \mu\left(\left(\frac{r\lambda x}{1+\lambda(1-x)^2}\right)(mod\ 1)\right) & for\ x < ½ \\ \mu\left(1 - \left(\frac{r\lambda x}{1+\lambda(1-x)^2}\right)(mod\ 1)\right) for\ x \geq ½ \end{cases} \quad (6)$$

Furthermore, this equation is called the MS Tent map chaotic function and can be represented in recursive form as shown in Eq. (7), for $= 0,1,2,3, \ldots$.

$$(x_{n+1}) = \begin{cases} \mu\left(\left(\frac{r\lambda x_n}{1+\lambda(1-x_n)^2}\right)(mod\ 1)\right) & for\ x_n < ½ \\ \mu\left(1 - \left(\frac{r\lambda x_n}{1+\lambda(1-x_n)^2}\right)(mod\ 1)\right) for\ x_n \geq ½ \end{cases} \quad (7)$$

III. RESULT AND ANALYSIS

The chaotic behavior of the proposed MS Tent map can be evaluated using three types of analysis. First is bifurcation diagram analysis for density sensitivity test. Second is Lyapunov exponent diagram analysis for transitive test and the last one is NIST Randomness tests using 16 statistical tests. These three tests are carried out on the number sequence or keystream generated by the MS Tent map. Algorithm 1 shows how to generate a keystream using the MS Tent map.

After testing the chaotic properties has been completed, the next stage is to develop encryption and decryption algorithms as shown by Algorithms 2 and 3. To analyze the results of the encrypted image and decrypted image, the keystream generated by MS Tent map is used with the initial value of the variable $x_0 = 0.9$ and the parameters $\lambda = 30$, $\mu = 1.5$, and $r = 3.7$. All algorithms keystream generator, keystream testing, image encryption and decryption are implemented using Python programming language and runed on a computer with the specification Intel(R) Core (TM) i5-4200M CPU @ 2.50GHz and 10.00 GB of Memory (RAM).

Performance analysis of the proposed chaotic function is carried out on encrypted and decrypted images using 30 test images: 15 color images and 15 grayscale images. To test the resistance of an encrypted image to brute force attacks, several indicators are used:

1) Sensitivity analysis.
2) Key space measurement analysis.
3) Correlation analysis.
4) Image quality test.

Algorithm 1: Keystream Generator Algorithm

Input: x_0, λ, μ, r, t
Output: *Keystream* K_i
1. For $i = 1\ to\ t\ do$
2. calculate x_i using Eq. (7)
3. $K_i \leftarrow \lfloor x_i \times 10^6 \rfloor mod\ 256$
4. End For

Algorithm 2: Image encryption algorithm

Input:x_0, λ, μ, r, t, original image ($P_i: m \times n$)
Output: encrypted image ($C_i: m \times n$)
1. $N = m \times n$; $i = 1$
2. If $i \leq N$, do Step-3 to step-6
3. Calculate x_{i+t} using Eq. (7)
4. $K_{i+t} \leftarrow \lfloor x_{i+t} \times 10^6 \rfloor \, mod \, 256$
5. $C_i = P_i \oplus K_{i+t}$
6. $i = i + 1$; Back to Step-2
7. Else to step-8
8. Show matrix C_i in encrypted image display

Algorithm 3: Image decryption algorithm

Input: x_0,r,λ,μ, i, t, encrypted image ($C_i: m \times n$)
Output: decrypted image ($D_i: m \times n$)
1. $N = m \times n$; $i = 1$
2. If $i \leq N$, do Step-3 to step-6
3. Calculate x_{i+t} using Eq. (7)
4. $K_{i+t} \leftarrow \lfloor x_{i+t} \times 10^6 \rfloor \, mod \, 256$
5. $D_i = C_i \oplus K_{i+t}$
6. $i = i + 1$; Back to Step-2
7. Else to step-8
8. Show matrix D_i in decrypted image display

A. Bifurcation Diagram

A bifurcation diagram is a diagram that shows the asymptotically approximate values of a system as the function of the parameters. By looking at the bifurcation diagram, we can determine the chaotic nature of a function. If the periodic points on the bifurcation diagram are dense, then the function is chaotic [2].

Algorithm 4. Plotting Bifurcation Diagram

Input: x_0, λ, μ, r, t
Output: plotting x_i
1. For $i = 1$ to n
2. Calculate x_i using Eq. (7)
3. Plotting x_i
3. end for

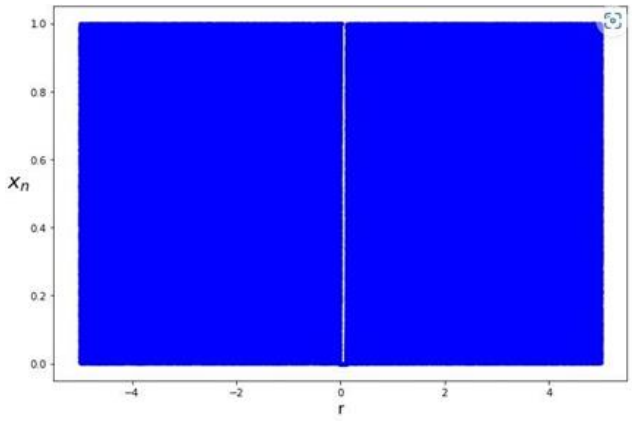


Fig. 1. MS Tent map bifurcation diagram, for $x_0 = 0.9$, $\lambda = 30$, $\mu = 1.5$, $r = 3.7$.

Based on Algorithm 4, with variable values of $x_0 = 0.9$, $\lambda = 30$, $\mu = 1.5$, $r = 3.7$, a diagram is obtained as seen in Fig. 1. The result of the bifurcation diagram is dense for every value of r except for $r = 0$. Thus, the MS Tent map has chaotic properties except for $r = 0$.

B. Lyapunov Exponent Diagram

According to Eq. (8), the Lyapunov exponent can measure the sensitivity of a chaotic system to initial conditions. The Lyapunov exponent is defined as the exponential difference in the divergence or convergence of two vectors in a plane starting from the area around the plane.

Definition: Let X be a set. The map $f : X \rightarrow X$ is chaotic on X, if f is sensitive on the initial value, f is topologically transitive, and the periodic points are dense on X [10].

A function f is said to be chaotic if its Lyapunov exponent is positive. The Lyapunov exponent equation is defined according to Eq. (8) and its implementation uses Algorithm 5. Fig. 2 is a plot result of the Lyapunov exponent diagram, which shows that the MS Tent map has positive Lyapunov exponents at $x_0 = 0.9$, $\lambda = 30$, and for every value of r except for $r = 0$. This proves that the MS Tent map has chaotic properties.

$$\mu = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} ln|f'(x)| \quad (8)$$

Algorithm 5. Lyapunov Exponent Diagram

Input: x_0, λ, μ, r
Output: plotting the value of μ
1. for $i = 1$ to n
2. Calculate μ using Eq. (8)
3. plotting μ
4. end for

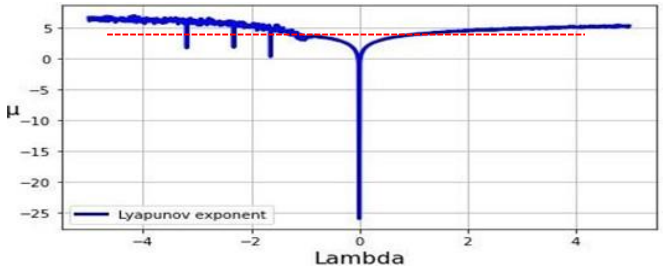


Fig. 2. Lyapunov exponent diagram of the MS Tent Map.

C. Key Stream Randomness Test

After conducting a chaotic test on the MS Tent map function using a bifurcation diagram and Lyapunov exponent, then a randomness test is carried out on the keystream or number sequence generated from this function. The keystream randomness test used is the NIST test suite which aims to evaluate the chaotic level of MS Tent map function [12]. The NIST test suite is a statistical package consisting of 16 tests [13] and their results are shown in the Table I. Based on these 16 statistical tests results, it can be concluded that the keystream generated by MS Tent map is random. This is because the statistical test process shows that the P-value is greater than the significance level (by default it is 0.01).

TABLE I. NIST RANDOMNESS TEST RESULTS OF THE MS TENT MAP

Type of Test	P-Value	Conclusion
Frequency (Monobit)	0.031555	Successful
Frequency within a Block	0.748768	Successful
Run Test	0.394557	Successful
Longest Run of Ones in a Block	0.229904	Successful
Binary Matrix Rank	0.168577	Successful
Discrete Fourier Transform (Spectral)	0.755036	Successful
Non-Overlapping Template Matching	0.425093	Successful
Overlapping Template Matching	0.904727	Successful
Maurer's Universal Statistical	0.803366	Successful
Linear Complexity	0.141618	Successful
Serial Test	0.356311	Successful
	0.490805	Successful
Approximate Entropy	0.083009	Successful
Cumulative Sums (Forward)	0.060013	Successful
Cumulative Sums (Reserve)	0.025765	Successful
Test Random Excursions	0.431326	Successful
Test Random Excursions Varian	0.641948	Successful

D. Sensitivity Analysis

Sensitivity analysis aims to find out how big the difference is between the key parameter values used in the encryption process and the key parameter values applied in the decryption process, so that they can be considered the same or different. Fig. 3 is two examples of color and grayscale face images used for sensitivity testing. In the image encryption process the parameters values employed are: $x_0 = 0.9$, $\lambda = 30$, $\mu = 1.5$, $r = 3.7$, and iteration $t = 100$.

The sensitivity test results are displayed in Table II. The tests are performed by varying the value of each parameter, as shown in the first and second columns. The third column displays the decrypted image results according to the parameter values used in the first and second columns. The last column represents the histogram pattern of each decrypted image in the third column.

The key variable x_0 has a sensitivity value of 10^{-17}. This is proven because for x_0 value with a difference of up to 10^{-17} the decrypted image has not returned to the original image and their histogram appears to have a uniform (flat) distribution. Visually from this histogram, one cannot predict what information is contained in the original image. The decrypted image will only return to the original if the difference between x_0 value in the encryption and decryption processes is 10^{-18}. The sensitivity levels of the other parameters are: $r = 10^{-17}$, $\lambda = 10^{-16}$, and $\mu = 10^{-17}$. Based on the sensitivity test results, it can be concluded that the encrypted image is safe against brute force attacks at the sensitivity level of each parameter: $x_0 = 10^{-17}$, $r = 10^{-16}$, $\lambda = 10^{-15}$, and $\mu = 10^{-16}$.

E. Key Space Measurement Analysis

Brute force attacks usually always try all possible keys to decrypt to get the actual facial image. To reduce the chance of a successful brute force attack, the algorithm must also have a large key space. The key space represents the number of different keys that can be used to perform encryption/decryption [14]. In Python, the maximum value of floating-point numbers is $1.7976931348623157\times10^{308} \approx 1.8\times10^{308}$. The natural numbers lie in the interval (0, 1), the precession rate reached $2^{52} \approx 10^{15}$ and the integer data had a possible value of $2^{64} \approx 1{,}8\times10^{19}$. The encryption and decryption algorithms based on MS Tent map chaotic function have five parameters: x_0, r, μ, λ, and iteration t with domains $x_n \in (0, 1)$, λ, μ, r, $\in$ R, and $t \in$ Z. Overall, these five parameters can produce a key space size of $1.8\times10^{308} \times 1.8\times10^{308} \times 1.8\times10^{308} \times 10^{15} \times 1.8\times10^{19} \approx 1.05\times10^{959}$. This key space is very large, so the encrypted image can be resistant to the brute force attacks.

(a) (b)

Fig. 3. (a) Color face image. (b) Grayscale face image.

TABLE II. SENSITIVITY TEST RESULTS FOR DIFFERENCES IN PARAMETER VALUES x_0, μ, r, λ

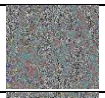
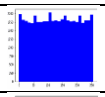
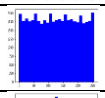
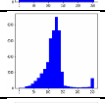
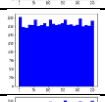
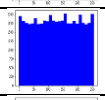
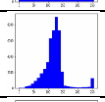
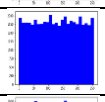
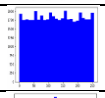
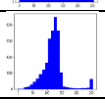
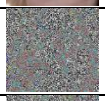
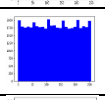
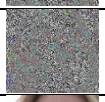
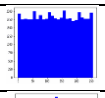
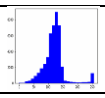
Sensitivity Test Results		Face Image Decryption	Histogram
Initial value difference x_0 with $r = 3.7$, $\mu = 1.5$, and $\lambda = 30$	$x_0 = 0.9 + 10^{-6}$		
	$x_0 = 0.9 + 10^{-17}$		
	$x_0 = 0.9 + 10^{-18}$		
Parameter value difference r with $x_0 = 0.9$, $\mu = 1.5$, and $\lambda = 30$	$r = 3.7 + 10^{-6}$		
	$r = 3.7 + 10^{-16}$		
	$r = 3.7 + 10^{-17}$		
Parameter value difference λ with $x_0 = 0.9$, $r = 3.7$, and $\mu = 1.5$	$\lambda = 30 + 10^{-6}$		
	$\lambda = 30 + 10^{-15}$		
	$\lambda = 30 + 10^{-16}$		
Parameter Value difference μ with $x_0 = 0.9$, $r = 3.7$, and $\lambda = 30$	$\mu = 1.5 + 10^{-6}$		
	$\mu = 1.5 + 10^{-16}$		
	$\mu = 1.5 + 10^{-17}$		

TABLE III. KEY SPACE COMPARISON OF CHAOTIC FUNCTIONS

Function	Parameters	Key Space
Tent Map [11]	$\boldsymbol{x}_n \in (0, 1)$, $\boldsymbol{\mu} \in \mathbb{R}$, and $t \in \mathbb{Z}$	1.8×10^{323}
MS Map [15]	$\boldsymbol{x}_n \in (0, 1)$, $\boldsymbol{\lambda}, \boldsymbol{r} \in \mathbb{R}$, $t \in \mathbb{Z}$	3.24×10^{635}
Tent + MS Map	$\boldsymbol{x}_n(t), \boldsymbol{x}_n(\mathbf{ms}) \in (0, 1)$, $\lambda, r \in \mathbb{R}$, $t \in \mathbb{Z}$	5.832×10^{958}
MS Tent Map	$\boldsymbol{x}_n \in (0, 1)$, $\boldsymbol{\lambda}, \boldsymbol{\mu}, r \in \mathbb{R}$, and $t \in \mathbb{Z}$	1.05×10^{959}
MS Circle Map [16]	$\boldsymbol{x}_n \in (0, 1)$, $\lambda, r, \Omega, K \in \mathbb{R}, t \in \mathbb{Z}$	1.889×10^{1267}

Table III displays the key space of chaotic functions, where the first and second rows represent the key space of the Tent map and MS map which are 1.8×10^{323} and 3.24×10^{635} respectively. The third row is a key space of 5.832×10^{958} which is produced when the encryption process is carried out twice serially by the Tent map and MS map. In the fourth row is a key space of 1.05×10^{959}, if the proposed MS Tent map is applied for the data encryption process. This shows that data encryption based on MS Tent Map is more secure against brute force attacks than when using MS Map, Tent Map and a serial combination of MS Map and Tent Map.

F. Correlation Analysis Test

Correlation analysis is a method used to determine the direction and strength of the relationship between two variables [17] or between pixels in an image. The correlation coefficient is usually a value without units which is located between 1 and -1. High correlation (close to 1) indicates a strong relationship between neighboring pixel values, so that it can describe the information contained therein. On the other hand, low correlation (close to 0) means that the relationship between neighboring pixels is weak, so that no information can be depicted by these pixels.

Table IV shows the results of the correlation coefficient test from color and grayscale images in Fig. 3. The correlation coefficient is calculated referring to the correlation between neighboring pixels vertically, horizontally, and diagonally. In the second, third and fourth columns, all correlation coefficient values are close to 1 for the original images. These values show a close correlation between pixels in the images, so that all information can be read visually. On the other hand, all the correlation coefficient values of the encrypted images in the fifth, sixth and seventh columns are close to 0. This indicates that there is no correlation between pixels in the encrypted images, so that no information can be read visually from these images. Likewise, this correlation coefficient results show that the encrypted images are secure against statistical attacks.

G. Encrypted Image Quality Test

Functional analysis of encryption and decryption algorithms based on the proposed MS Tent map aims to determine their success in securing data: from the original images to the cipher images (encrypted images) and then returned to the original images (decrypted images), as demonstrated in the Fig. 4. In column (a) are the original images, in column (b) are the results of the encryption algorithm, and the results of the decryption algorithm can be found in column (c). In this functional analysis, it will be determined whether the decrypted images, as the results of the decryption process of the encrypted images, are the same as the original images.

(a) (b) (c)

Fig. 4. (a) Original images. (b) Encrypted images. (c) Decrypted images.

Mean Square Error (MSE) in Eq. (9) and Peak Signal to Noise Ratio (PSNR) in Eq. (10) are employed to measure the quality of the decrypted image compared to the original image. Quality analysis was carried out using thirty test images consisting of fifteen color images and fifteen grayscale images. These images have various colors, shapes, and textures features, as well as different sizes. The images in Fig. 4 are two of thirty test images.

$$PSNR(x, y) = 10 \log \frac{255^2}{MSE(x,y)} \quad (9)$$

$$MSE(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)^2 \quad (10)$$

Table V shows the MSE and PSNR values calculated between the original image and the decrypted image on thirty test images. MSE has a value of 0 and PSNR equals to ∞, for all decrypted color images (test image 1 to 15) and decrypted grayscale images (test image 16 to 30). These MSE and PSNR values prove that there are no errors in the decrypted images, or it can be said that the decrypted images are the same as the original images.

TABLE IV. CORRELATION COEFFICIENT TEST RESULTS OF COLOR AND GRAYSCALE IMAGES IN FIG. 3 AND THEIR ENCRYPTION

Test Data	Original Image Correlation Coefficient			Encrypted Image Correlation Coefficient		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Color faceimage	0.9885	0.9933	0.9827	0.00065	0.00019	0.0014
Grayscale face image	0.9525	0.9631	0.9246	0.0067	0.0017	0.0036

TABLE V. MSE AND PSNR VALUE BETWEEN THE ORIGINAL AND DECRYPTED IMAGES

Test Image	MSE	PSNR		Test Image	MSE	PSNR
1	0	∞		16	0	∞
2	0	∞		17	0	∞
3	0	∞		18	0	∞
4	0	∞		19	0	∞
5	0	∞		20	0	∞
6	0	∞		21	0	∞
7	0	∞		22	0	∞
8	0	∞		23	0	∞
9	0	∞		24	0	∞
10	0	∞		25	0	∞
11	0	∞		26	0	∞
12	0	∞		27	0	∞
13	0	∞		28	0	∞
14	0	∞		29	0	∞
15	0	∞		30	0	∞

IV. CONCLUSION

MS Tent map is a proposed chaotic function which is developed through the composition process of the two chaotic functions MS Map and Tent Map. Through sensitivity, transitivity, and randomness tests on the keystream generated by MS Tent map, it is proven that this function has chaotic properties. MS Tent map has four key parameters that can produce a key space of 1.05×10^{959}. This shows that data encryption based on MS Tent map is more secure against brute force attacks than when using MS map or Tent map or a serial combination of MS map and Tent map, which have key spaces of 1.8×10^{323}, 3.24×10^{635}, and 5.832×10^{958}, respectively. Likewise, based on the results of the correlation coefficient analysis, it shows that encrypted images are also secure against statistical attacks.

REFERENCES

[1] I Kadek Aldy Oka Arditaa, Agus Muliantara, I Gusti Ngurah Anom Cahyadi Putra, Ngurah Agus Sanjaya ER, Ida Bagus Made Mahendra, I Wayan Supriana, Enkripsi Gambar Berdasarkan Modifikasi Bit Piksel Dengan Menggunakan Perpaduan Logistic Map Dan Henon Map. *Jurnal Elektronik Ilmu Komputer Udayana*, Volume 11, No 2. November 2022.

[2] L. Kocarev, S. Lian, *Chaos-based cryptography: Theory, algorithms, and applications*. Springer-Verlag, Berlin, 2011.

[3] Eva N., & Suryadi M.T. Chaos-Based Encryption Algorithm for Digital Image. *Proceeding IICMA 2013*, Yogyakarta, 2014, pp. 169-177.

[4] Suryadi M. T., Eva N., and Dhian W. Performance of Chaos-Based Encryption Algorithm for Digital Image. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, 2014, 12(3): 675-682.

[5] Suryadi M. T., Maria Y. T. I., and Satria Y. Encryption Algorithm using New Modified map for digital image. *Journal of Physisc: Conference Series*, 2017, 893: 012050.

[6] Dai, Yin, and Xin Wang. Medical image encryption based on a composition of logistic maps and chebyshev maps. *2012 IEEE international conference on information and automation*. IEEE, 2012.

[7] Suryadi, M.T, Satria, Y. & Prawadika, L. N., An improvement on the chaotic behavior of the gauss map for cryptography purposes using the circle map combination, *Journal of Physics: Conference Series*, Vol. 1490, IOP Publishing, 2020, p. 012045.

[8] Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang. Image Encryption with Double Spiral Scans and Chaotic Maps. *Hindawi Security and Communication Networks*, 2019.

[9] Arthi, G. and Thanikaiselvan, V. and Amirtharajan, R., 4D Hyperchaotic map and DNA encoding combined image encryption for secure communication. *Multimedia Tools and Applications*, 2022.

[10] N. K Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map. *Journal of Image and Vision Computing*, 24 (2006).

[11] Chunhu Li, Guangchun Luo, Ke Qin & Chunbao Li, Animage encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, 87.1 (2017), pp. 127–133.

[12] Suryadi MT, MYT Irsan, S Yudi, New modified map for digital image encryption and its performance. *Journal of Physisc: Conference Series*, 893, 1 (2017).

[13] A. Rukhin, J. Soto, j. Nechvatal, E. Barker, S. Leigh, *A Statistical test suite for random and pseudorandom number generators for cryptographic applications*. NIST Special publication (2010).

[14] Fu, C., Chen, J.-j., Zou, H., Meng, W.-h., Zhan, Y.-f. & Yu, Y.-w., A chaos-based digital image encryption scheme with an improved diffusion strategy, *Optics express* 20(3), 2363–2378, 2012.

[15] Suryadi M T, Maria Y T I, and Yudi S (2016). New Modified Map for Digital Image Encryption and Its Performance. *Proceedings The Asian Mathematical Conference* 2016 (2016).

[16] Suci Boru Kembaren, Suryadi M.T., Triswanto. Implementasi Algoritma Enkripsi Citra Digital Berbasis Chaos Menggunakan Fungsi Komposisi Logistic Dan Gauss Iterated Map. *Prosiding Seminar Nasional & Internasional*, Vol. 1 (2018).

[17] Walpole, R. E. & Ergle, W. D., *Elementary statistical concepts*, MacMillan Basingstoke,1983.