Nonlinear Dynamics and Systems Theory, **23** (5) (2023) 545–560

Moore-Spiegel Chaotic Encryption for Digital Images and Voices

W. S. M. Sanjaya [1,2*], A. Roziqin [3], A. W. Temiesela [1], M. F. B. Zaman [1], A. D. Wibiksana [1] and D. Anggraeni [1,2]

[1] *Department of Physics, Faculty of Science and Technology, UIN Sunan Gunung Djati, Bandung, Indonesia.*
[2] *Bolabot Techno Robotic Institute, CV Bolabot, Bandung, Indonesia.*
[3] *Department of Madrasah Ibtidaiyah Teacher Edu., Faculty of Education and Teaching, UIN Sunan Gunung Djati, Bandung, Indonesia.*

Received: June 20, 2023; Revised: November 11, 2023

Abstract: In this study, we explore the application of the Moore-Spiegel chaotic system in both image and voice encryption, considering the increasing importance of data security in the digital age. The analysis of the chaotic system involves examining phase diagrams, time series, bifurcation diagrams, Lyapunov exponent analysis, and Poincaré maps to understand its dynamics. For image encryption, we evaluate the system's effectiveness through various analyses, including histogram analysis, correlation analysis, entropy analysis, NPCR and UACI analysis, and noise attack analysis. Similarly, for voice encryption, we assess it through various analyses, including waveform plots, FFT, spectrograms, correlation coefficients, entropy analysis, and RMSE. The findings demonstrate the suitability of the Moore-Spiegel chaotic system for both image and voice encryption, suggesting its potential as a data transmission masking technique. The research includes numerical simulations conducted using Python to support the proposed approach.

Keywords: *Moore-Spiegel chaotic system; chaotic analysis; voice encryption; masking method; image encryption; XOR method.*

Mathematics Subject Classification (2010): 94A60, 37D45, 34F10, 74H65, 34D08, 94A08, 94A12.

* Corresponding author: mailto:madasws@gmail.com;~mada.sanjaya@uinsgd.ac.id

1 Introduction

In recent times, ensuring the security and integrity of data transmitted through communication systems has become a significant focus for scientists. Research on chaos over the past four decades has revealed its complex and unpredictable behavior in various domains such as physics, climatology, chemistry, and biology. [1]

The Moore-Spiegel system, discovered in 1966, is a chaotic system that describes aperiodic dynamics and has applications in understanding thermal dissipation and convectively unstable fluids [2]. In 2017, the Moore-Spiegel synchronization circuit was applied to a communication security system [3].

Numerous studies have explored the application of chaotic systems in encryption, including image encryption using 1D, 2D, and 3D chaotic systems [4–6], as well as voice encryption using the Jerk, Chua, and Bhalekar-Gejji chaotic systems [7–9]. While the previous research demonstrates the potential of chaotic systems in encryption, further optimization and security analysis are required.

This paper is structured as follows. Section 2 discusses the analysis of the Moore-Spiegel Chaotic System, including phase diagrams, time series, bifurcation analysis, Lyapunov exponent analysis, and Poincaré analysis. Section 3 explains the encryption and decryption algorithms for digital images and voice using the Moore-Spiegel system. Section 4 presents experimental results and analysis. For image encryption, we perform histogram analysis, correlation analysis, entropy analysis, NPCR and UACI analysis, and noise attack analysis. For voice encryption, we conduct voice signal plot analysis, correlation coefficient analysis, voice entropy analysis, and Root Mean Squared Error (RMSE) analysis. Finally, Section 5 concludes and provides a final assessment.

2 Moore-Spiegel Chaotic System and Basic Analysis

The Moore-Spiegel system is described by the following system of differential equations:

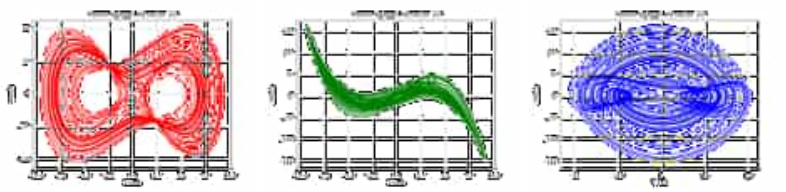
$$\begin{cases} \dot{x} &= y, \\ \dot{y} &= z, \\ \dot{z} &= -z + ay - x^2 y - bx. \end{cases} \tag{1}$$

The parameters and the initial conditions of Moore-Spiegel chaotic system are chosen as: $a = 9$, $b = 5$, and $(x_0, y_0, z_0) = (2, 7, 4)$ so that the system shows the expected chaotic behavior [2, 3, 10].

2.1 Phase diagram and time series

The signal plots of the Moore-Spiegel chaotic system with the constant parameters $a = 9$ and $b = 5$, and the initial condition of (2, 7, 4) were simulated using Python 3, as depicted in Figure 1. The corresponding phase diagrams are illustrated in Figure 1. The graphs obtained from the Moore-Spiegel system equations exhibit chaotic behavior, indicating their suitability for digital image and voice encryption.

The utilization of phase diagrams and time series diagrams provides a solution for analyzing the Moore-Spiegel system's differential equation. These diagrams allow the observation of the system's movement characteristics. By examining the time series plot of variables x, y, and z in Figure 2, it becomes evident that the Moore-Spiegel system exhibits chaotic behavior.



(a) (b) (c)

Figure 1: The 2D phase diagram of the Moore-Spiegel chaotic system; (a) y vs x, (b) z vs x, (c) z vs y, with the parameter values $a = 9$, and $b = 5$.

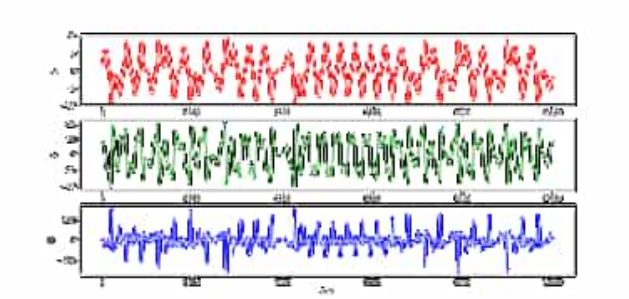
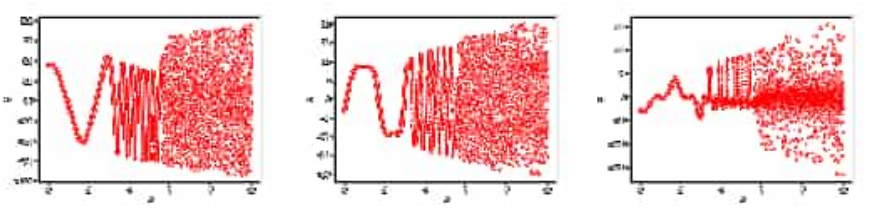


Figure 2: The time series for the Moore-Spiegel chaotic system with the parameter values $a = 9$ and $b = 5$.

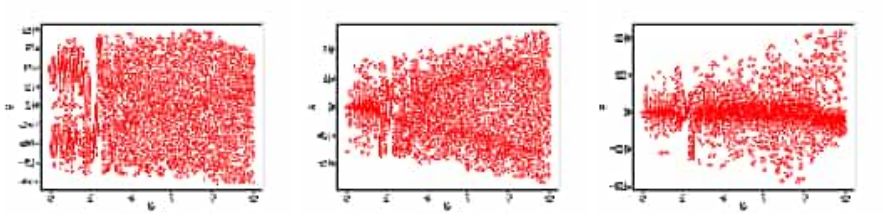
2.2 Bifurcation analysis

The bifurcation diagram represents the transition of a discrete dynamical system from regular behavior to chaos [11]. Bifurcation analysis was carried out for the Moore-Spiegel chaotic system using a fixed set of parameter values, starting from the initial condition of (2, 7, 4). We perform 10,000 iterations with a time step of 0.01. The findings depicted in Figure 3 illustrate the bifurcation diagram of the Moore-Spiegel system for the parameter values within the range of $5.0 \leq a \leq 10.0$, revealing the presence of chaotic dynamics with periodic patterns. Similarly, Figure 4 illustrates the occurrence of chaotic behavior with periodic patterns in the system when the parameter value falls within the range of $3.0 \leq b \leq 10.0$.



(a) (b) (c)

Figure 3: Bifurcation diagram with the parameters $b = 5$ and $a =$ varied; (a) x vs a, (b) y vs a, (c) z vs a.



(a) (b) (c)

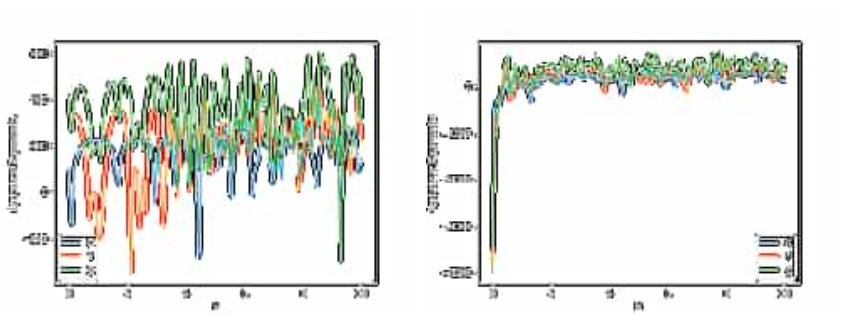
Figure 4: Bifurcation diagram with the parameters $a = 9$, and $b =$ varied; (a) x vs b, (b) y vs b, (c) z vs b.

2.3 Lyapunov exponent

The Lyapunov exponent (λ_V) is a metric employed in the realm of dynamical systems theory to gauge how susceptible a system is to alterations in its initial conditions. We employed a predefined set of parameter values and initialized the simulation with an initial state of (2, 7, 4). Following that, we conducted 10,000 iterations with a time increment of 0.01. Within the framework of the Moore-Spiegel chaotic system equations, the variable $v_i(a,\ b)$ signifies the value of the x, y, or z component at time step i within a simulation carried out with specific parameter values a, and b [12, 13]. The equation for the Lyapunov Exponent is stated as follows:

$$\lambda_V(a,\ b) = \frac{1}{dt} \ln \left(\frac{1}{N} \sum_{i=0}^{N-1} |v_i(a,\ b)| \right). \tag{2}$$

The Lyapunov exponent formula allows us to understand the extent to which the Moore-Spiegel chaotic system is sensitive to changes in its initial conditions and whether the system tends toward chaotic or stable behavior over time. The strange attractor shows three Lyapunov exponents with positive, zero, and negative values [3].



(a) (b)

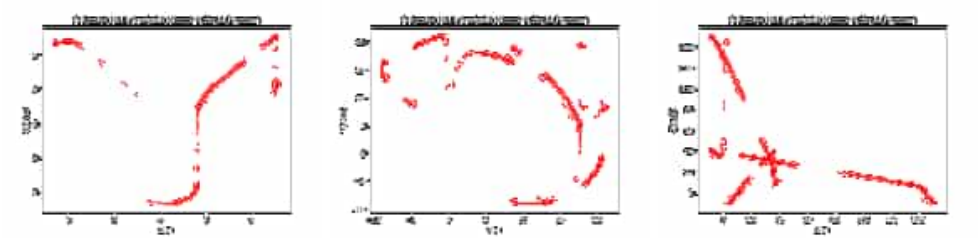
Figure 5: The Lyapunov exponents when the parameters are varied as follows: (a) $b = 5$ and $a =$ varied, (b) $a = 9$ and $b =$ varied.

Figure 5 illustrates chaotic behavior in the range of $5.0 \leq a \leq 10.0$, with other parameters held constant. The diagram displays periodic patterns amidst the chaos.

Furthermore, within the range of $3.0 \leq b \leq 10.0$, while keeping the other parameters constant, the system exhibits diverse chaotic behaviors for different parameter values, specifically $a = 9$ and $b = 5$. The system demonstrates limit point behavior due to the presence of two negative Lyapunov exponents.

2.4 Poincare analysis

The Poincaré map provides insights into periodic and non-periodic systems. Periodic systems exhibit a limited number of points with a repetitive structure, while non-periodic systems have a larger number of points with an unpredictable structure, with some points repeating.



(a) (b) (c)

Figure 6: Poincare map with the parameters $a = 9$, and $b = 5$; (a) $x(n+1)$ vs $x(n)$, (b) $y(n+1)$ vs $y(n)$, (c) $z(n+1)$ vs $z(n)$.

Figure 6 shows the Poincaré map for the Moore-Spiegel system, where $a = 9$ and $b = 5$. The map demonstrates chaotic behavior in the Moore-Spiegel chaotic system. It is characterized by scattered points with an irregular structure, and some points show repetition. The Poincaré map helps understand qualitative features of strange attractors during chaotic states by revealing dense intersections and different trajectories in each period. Analyzing the Poincaré map is crucial to comprehend the attractors' qualitative characteristics.

3 The Moore-Spiegel System Algorithm

3.1 Encryption algorithm

Input (Image) : Original Image (Bird, Landscape, Cat)
Input (Voice) : Original Voice
Output (Image) : Encrypted Image
Output (Voice) : Encrypted Voice

- Step 1: Import the required libraries.
- Step 2: To generate the pseudo-random key, you can create a function named "secret-key" that utilizes the Moore-Spiegel chaotic system. For instance, you can select a solution from differential equation (1) that demonstrates chaotic behavior, such as x, y, or z, and use it as the basis for generating the pseudo-random key.

- Step 3: Specify the initial conditions and the "num" parameter responsible for inducing chaos in accordance with differential equations (1). As an illustration, you can set the initial condition to $(x,\ y,\ z) = (2,\ 7,\ 4)$ and use parameters $a = 9$ and $b = 5$.
- Step 4 (Image): Load the decrypted image and extract its height and width to be used in the "secret key" function.
- Step 4 (Voice): Read the voice file and convert the voice data into NumPy array format.
- Step 5: Iterate through each pixel (Image) or frame (Voice) in a loop.
- Step 6: Apply the XOR operation to encrypt the pixel (Image) or frame (Voice) using the pseudo-random numbers generated from the "secret key".
- Step 7: Obtain the encrypted image or encrypted voice.

3.1.1 Decryption algorithm

Input (Image) : Encrypted Image
Input (Voice) : Encrypted Voice
Output (Image) : Decrypted Image (Bird, Landscape, Cat)
Output (Voice) : Decrypted Voice

- Step 1: Import the required libraries.
- Step 2: Read the encrypted image or encrypted voice file and extract its dimensions or transform the voice data into a NumPy array.
- Step 3: Define the initial values and the "num" parameter that result in chaotic characteristics, similar to those in the encryption system. For instance, establish the initial condition as $(x,\ y,\ z) = (2,\ 7,\ 4)$, with parameters $a = 9$ and $b = 5$.
- Step 4: Produce a pseudo-random key through the development of a function named the "secret-key" that leverages the Moore-Spiegel chaotic system. For instance, opt for a solution within differential equation (1), be it x, y, or z, that demonstrates chaotic behavior to serve as the basis for the pseudo-random key.
- Step 5: Iterate through each pixel in the encrypted image or frame in the encrypted voice file.
- Step 6: Decrypt the pixel (Image) or frame (Voice) by performing XOR operation between the encrypted pixel (Image) or frame (Voice) and the corresponding pseudo-random number from the secret key.
- Step 7: Obtain the decrypted image or decrypted voice.

4 Experiment Results

In this section, we divide the experimental results into two parts: image encryption and voice encryption.

4.1 Image encryption

In this part, we conducted an evaluation of the Moore-Spiegel chaotic system's masking approach, utilizing three unique images: Bird, Landscape, and Cat. Our analysis was primarily focused on appraising the system's effectiveness in encrypting and ensuring the security of image files, as shown in Figure 7.

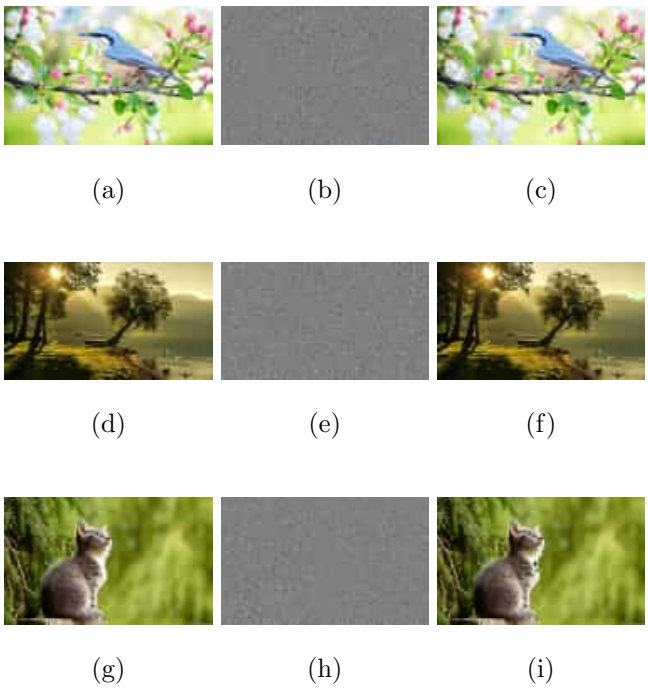
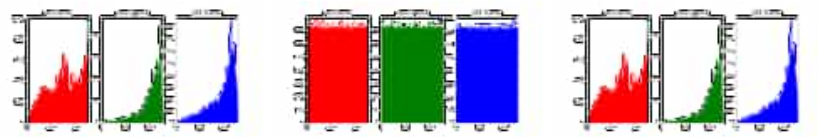


Figure 7: Application of the Moore-Spiegel chaotic system in Digital Image Encryption and Decryption. **(a, d, g)** Original. **(b, e, h)** Encrypted. **(c, f, i)** Decrypted.

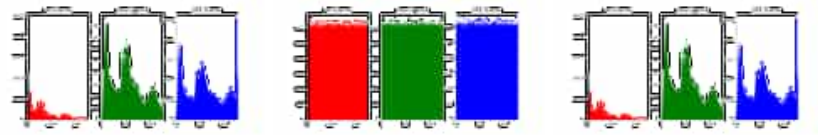
4.1.1 Histogram image encryption analysis

Histogram analysis portrays the distribution of pixel intensities graphically in an image. It provides insights into the prevalence of different ranges of pixel intensities [14]. Pixels in an original image have distinct and information rich diagonal bars. These diagonal bars are vulnerable to attacks. To counter such attacks, the encryption algorithm should ensure that the encrypted image has evenly distributed bars [15]. Figure 8, 9, 10 show histogram analysis results for the original image, encrypted image, and decrypted image. The original image's histogram displays non-flat distribution with clustering tendencies on the left and right sides. The histogram of the encrypted image indicates a successful encryption with a flat distribution. The histogram of the decrypted image demonstrates a successful decryption, restoring a similar distribution as in the original image.



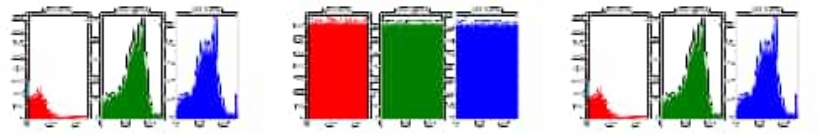
(a) (b) (c)

Figure 8: Histogram analysis of Bird image: (a) original, (b) encrypted, (c) decrypted.



(a) (b) (c)

Figure 9: Histogram analysis of Landscape image: (a) original, (b) encrypted, (c) decrypted.



(a) (b) (c)

Figure 10: Histogram analysis of Cat image: (a) original, (b) encrypted, (c) decrypted.

4.1.2 Correlation image encryption analysis

Correlation analysis measures the degree of correlation between multiple images using a correlation coefficient ranging from -1 to 1. A correlation coefficient of 1 represents a perfect positive relationship, 0 indicates no relationship, and -1 represents a perfect negative relationship [1]. The correlation coefficient is calculated based on the relative ranking of pixel intensities in the images, rather than their actual values. It can be expressed mathematically as follows:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{(D(x)D(y))}}, \tag{3}$$

where

$$Cov(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))(y_j - E(y)), \tag{4}$$

$$E(x) = \frac{1}{N}\sum_{j=1}^{N} X_j, \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - E(x))^2. \tag{6}$$

The correlation coefficient equation involves the expected values of variables x and y denoted by $E(x)$ and $E(y)$, respectively. The term Cov represents the covariance between the variables, while $D(x)$ and $D(y)$ indicate the standard deviations of x and y. The variables x_j and y_j refer to the individual pixels in the first and second images, and N represents the total number of pixels involved in the calculation [1].

Image	**Channel**	**Original-Encrypted**	**Original-Decrypted**
Bird	R	-0.0056	1.0000
	G	0.0288	0.9999
	B	-0.0078	1.0000
	Average	0.0052	1.0000
Landscape	R	-0.0230	0.9999
	G	-0.0308	0.9999
	B	0.0279	1.0000
	Average	-0.0087	0.9999
Cat	R	0.0036	1.0000
	G	0.0217	1.0000
	B	0.0236	0.9999
	Average	0.0163	1.0000

Table 1: Image correlation analysis.

Table 1 presents the results of correlation analysis conducted for the encrypted image and decrypted image of the three images using RGB analysis. The correlation coefficients between the pixels of the original images and the encrypted images are close to zero, indicating a lack of correlation and successful image masking. On the other hand, the correlation coefficients between the pixels of the original images and those of the decrypted images show a perfect correlation, confirming the algorithm's successful execution.

4.1.3 Entropy image encryption analysis

Image entropy within the RGB channels serves as a statistical metric employed to evaluate the degree of uncertainty or randomness present in the distribution of pixel values within each individual color channel (namely, Red, Green, and Blue) in the color image. Entropy offers insights into the uniformity or concentration of information within each channel. A heightened entropy value implies a more haphazard distribution of pixel values, whereas a lower entropy value signifies a more structured or concentrated arrangement of color distribution [16]. The calculation for determining the information entropy value is defined by the following equation:

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log_2(p(x_i)), \tag{7}$$

in this context, $H(X)$ stands for the entropy measure of the probability distribution X, $p(x_i)$ signifies the likelihood of pixel value x_i occurring within the distribution, N corresponds to the total count of unique pixel values in the distribution, and $\log_2(p(x_i))$ denotes the logarithm base-2 of the probability associated with pixel value x_i.

Based on Table 2, the entropy value for the encrypted image is higher than those for the original and decrypted images. The higher the entropy value (closer to 8), the higher the level of disorder in the information content of the image. This means that the information contained in the encrypted image is irregular, random, and difficult to comprehend.

Image	Channel	Original	Encrypted	Decrypted
Bird	R	7.35329	7.99193	7.35329
	G	7.07455	7.99194	7.07455
	B	7.83513	7.99198	7.83513
Landscape	R	7.84448	7.99202	7.84448
	G	7.80162	7.99197	7.80162
	B	7.04028	7.99200	7.04028
Cat	R	7.55674	7.99196	7.55674
	G	7.55905	7.99203	7.55905
	B	6.94755	7.99195	6.94755

Table 2: Image entropy values.

4.1.4 NPCR and UACI Analysis

1. **NPCR (Normalized Pixel Change Rate):** The NPCR (Normalized Pixel Change Rate) calculates the proportion of the pixel alterations between two images that have undergone encryption or decryption procedures. This parameter offers insight into the extent of pixel modifications that occur as a result of applying encryption or decryption algorithms [17] calculated by

$$\text{NPCR} = \frac{\text{Number of Changed Pixels}}{N \times M} \times 100\%, \tag{8}$$

where N and M represent the dimensions of the image in pixels, and the "Number of Changed Pixels" is the count of pixel positions where the pixel values differ between the two images.

2. **UACI (Unified Average Changing Intensity):** UACI quantifies the mean intensity variation between two images that are being compared. Intensity change is assessed by calculating the absolute difference between pixel values in the first and second images, and this value is then averaged across all pixels. UACI offers insights into the degree of intensity alterations that take place following an encryption or decryption process [17]. The UACI is computed using the following formula:

$$\text{UACI} = \frac{\text{Sum of Intensity Differences}}{N \times M \times L} \times 100\%, \tag{9}$$

where N and M stand for the pixel dimensions of the image, L signifies the total number of potential intensity levels for each pixel, which is typically 256 for an 8-bit image. The "Sum of Intensity Differences" corresponds to the summation of absolute disparities between corresponding pixel values in the two images.

In Table 3, the NPCR (%) column depicts the percentage of pixel changes between the original image and the encrypted image, as well as between the original image and the

decrypted image. The research results indicate significant pixel changes in the encrypted image, with percentages of approximately 98.50 %, 97.32 %, and 97.99 %, highlighting a noticeable transformation in the encrypted image compared to the original one.

Image	**NPCR (%)**		**UACI (%)**	
	Original - Encrypted	**Original - Decrypted**	**Original - Encrypted**	**Original - Decrypted**
Bird	98.50 %	0.00 %	30.81 %	0.00 %
Landscape	97.32 %	0.00 %	29.65 %	0.00 %
Cat	97.99 %	0.00 %	23.32 %	0.00 %

Table 3: NPCR and UACI percentages.

Meanwhile, the UACI (%) column of Table 3 illustrates the percentage of the pixel intensity changes between the original image and the encrypted image, as well as between the original image and the decrypted image. The research findings also reveal significant fluctuations in pixel intensity within the encrypted image. However, the decryption process successfully restores the image to its original pixel intensity levels, as evidenced by a UACI value of 0.00 % for all images. These findings provide an understanding of the impact of encryption and decryption algorithms on pixel changes and pixel intensity changes in the evaluated images.

4.1.5 Noise of attack image encryption analysis

The transmission of images may introduce distortions that can impact the final results. Therefore, it is crucial to evaluate the algorithm's performance against distortion attacks. The Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are utilized to measure the impact of noise on the decrypted image [18]. The equations for calculating the MSE and PSNR are as follows:

$$\text{PSNR} = 10 \log 10 \left(\frac{Max_i^2}{\text{MSE}} \right), \tag{10}$$

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (P_{ij} - C_{ij})^2. \tag{11}$$

In the given statement, P_{ij} represents the pixel value at the position i, j of the image without noise. C_{ij} represents the pixel value at the position i, j of the image with noise. Max_i denotes the maximum pixel value in the image.

We used density variations to modify the impact of noise. The MSE values were calculated by comparing the decrypted image after incorporating Salt and Pepper noise. A higher PSNR value indicates less information loss, while a higher MSE value indicates more information loss. In Table 4, it can be observed that at a density of 0.10, the MSE value is higher and the PSNR value is lower. Conversely, at a density of 0.05, the MSE value is lower and the PSNR value is higher.

Image	Variation of Density	MSE	PSNR
Bird	0.05	1148.51	17.53 dB
	0.10	2300.34	14.51 dB
Landscape	0.05	1131.49	17.59 dB
	0.10	2256.74	14.60 dB
Cat	0.05	1031.23	18.00 dB
	0.10	2062.23	14.99 dB

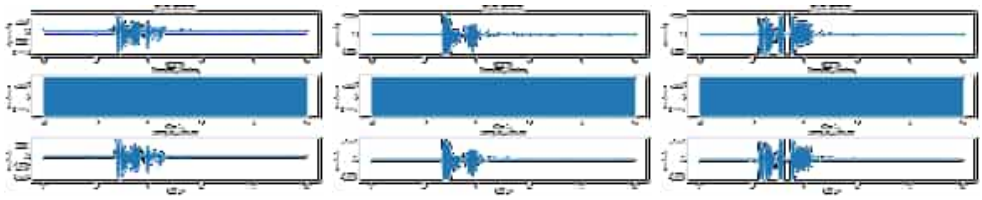
Table 4: The MSE and PSNR values were calculated for the decrypted image with salt and pepper noise.

4.2 Voice encryption

In this section, we tested the Moore-Spiegel chaotic masking system on three original voice files to ensure robust encryption, preserving confidentiality and integrity against unauthorized access and tampering.

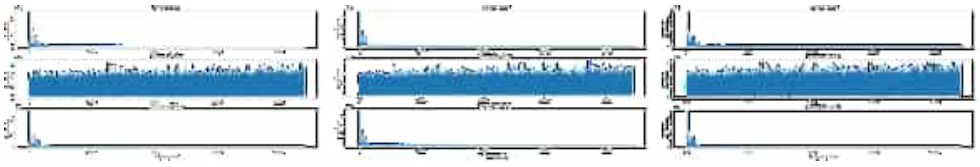
4.2.1 Voice signal plot

Waveform plots visually represent the signal's amplitude changes over time, aiding interpretation. Each frame of the voice signal is then transformed from time to frequency domain using FFT, enabling the analysis of voice characteristics such as high and low frequencies and amplitude strength at each frequency. Spectrogram plots display the signal's frequency against time and are shown sequentially in Figures 11, 12, and 13.



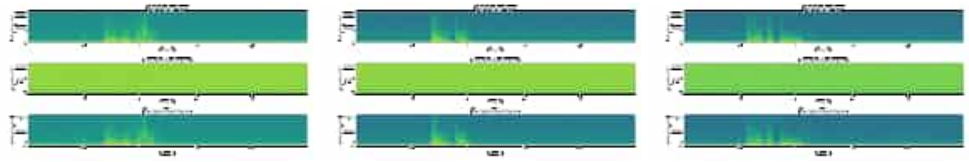
(a) (b) (c)

Figure 11: Waveform graph; (a) voice 1 ("*Terima Kasih*" in Bahasa), (b) voice 2 ("Thank You" in English), (c) voice 3 ("*Arigatou*" in Japanese).



(a) (b) (c)

Figure 12: FFT graph; (a) voice 1 ("*Terima Kasih*" in Bahasa), (b) voice 2 ("Thank You" in English), (c) voice 3 ("*Arigatou*" in Japanese).



(a) (b) (c)

Figure 13: Spectrogram graph ; (a) voice 1 ("*Terima Kasih*" in Bahasa), (b) voice 2 ("Thank You" in English), (c) voice 3 ("*Arigatou*" in Japanese).

The three images show Waveform, FFT, and Spectrogram graphs for the original voice, encrypted voice, and decrypted voice, respectively, for three different voices: voice 1 (Bahasa: "*Terima Kasih*"), voice 2 (English: "Thank You"), and voice 3 (Japanese: "*Arigatou*"). The analysis reveals that the encrypted voice signal has a distinct pattern, while the decrypted voice signal closely resembles the original voice signal. This demonstrates the algorithm's effectiveness in preserving the high quality of the recovered voice signal.

4.2.2 Correlation voice encryption analysis

The correlation analysis in voice encryption is governed by equations (3), (4), (5), (6). For voice encryption, the correlation analysis is performed with a similar methodology which differs in terms of the parameters used. $Cov(x, y)$ represents the covariance between the original signal x and the encrypted signal y. $D(x)$ and $D(y)$ denote the variances of signals x and y, respectively. N represents the number of voice samples. A low value of the correlation coefficient r_xy indicates a high-quality encryption [19].

Voice File	Original-Encrypted	Original-Decrypted
recording1.wav (*Terima Kasih*)	-0.00389	1.0
recording2.wav (Thank You)	-0.00055	1.0
recording3.wav (*Arigatou*)	-0.00079	1.0

Table 5: Voice correlation analysis.

The correlation coefficients between the original and encrypted voice signals are close to 0, indicating a lack of correlation, while the correlation coefficients between the original and decrypted voice signals are close to 1, indicating a strong correlation. Please refer to Table 5 for the specific values.

4.2.3 Entropy voice encryption analysis

In the realm of audio, entropy serves as a statistical metric employed to gauge the degree of uncertainty or randomness present in the arrangement of audio sample values. A heightened audio entropy signifies an increased diversity in audio sample values, potentially indicating the presence of more intricate or unpredictable sounds. Conversely, reduced entropy implies that the sound typically exhibits patterns or repetitions, with limited fluctuations in sample values [20].

The computation of audio entropy can be accomplished through Shannon's entropy formula, which is articulated as follows:

$$H(X) = -\sum_{i=1}^{N} p(x_i) \log_2(p(x_i)). \tag{12}$$

In this formula, $H(X)$ denotes the entropy of the probability distribution X representing audio sample values, $p(x_i)$ stands for the likelihood of occurrence of audio sample value x_i within the distribution, and N signifies the count of distinct audio sample values in the distribution. The provided algorithm calculates entropy for three different audio files: the original voice recording, the encrypted voice, and the decrypted voice. This program proves to be invaluable in the analysis of how audio information undergoes transformation during encryption and decryption procedures, shedding light on the complexity or randomness level of the audio files. A higher entropy value indicates a greater degree of variation in sample values within the audio.

Voice File	**Original**	**Encrypted**	**Decrypted**
recording1.wav (*Terima Kasih*)	11.33927	15.76719	11.33927
recording2.wav (Thank You)	11.45686	15.76808	11.45686
recording3.wav (*Arigatou*)	11.69892	15.76718	11.69892

Table 6: Voice entropy value.

The findings derived from the Shannon Entropy table, as presented in Table 6, elucidate that the encryption procedure exerts a substantial influence on the degree of unpredictability or randomness inherent in the audio data. This is evidenced by the notable escalation in Shannon Entropy values following the encryption process. However, subsequent to the decryption phase, the audio data regains a level of unpredictability akin to its original state, signifying the successful preservation of the fundamental information within the audio data. This inference suggests that, within this specific context, the encryption-decryption process can furnish additional security measures against unauthorized access to audio data while upholding the integrity of the data encapsulated within the audio files.

4.2.4 Root mean squared error (RMSE)

The RMSE (Root Mean Squared Error) measures the deviation between the predicted and actual values. A lower RMSE value is desirable as it indicates higher accuracy in the model's predictions. The ideal RMSE value depends on the specific problem and data range. While there is no universally defined ideal value, a decreasing RMSE signifies improved accuracy in the prediction model.

$$RMSE = \sqrt{\sum \frac{(x_{\text{pred}} - x_{\text{act}})^2}{N}}, \tag{13}$$

where x_{pred} is a predicted value, x_{act} is an actual value and N is the total data. Table 7 shows the comparison of RMSE values for voice decryption using low-level noise, indicating that the algorithm performs well.

Voice File	Variaty Density	RMSE
recording1.wav (*Terima Kasih*)	0.10	0.1002
	0.01	0.0100
recording2.wav (Thank You)	0.01	0.1002
	0.01	0.0100
recording3.wav (*Arigatou*)	0.10	0.1001
	0.01	0.0100

Table 7: The RMSE values for decrypted voice with Gaussian noise.

5 Conclusion

The previous research on the Moore-Spiegel system in communication security was limited to synchronization circuits, without applying it to image and voice encryption. Analysis shows that the Moore-Spiegel chaotic system is ideal for data encryption due to its unpredictability, randomness, and sensitivity to initial conditions, making it suitable for generating random encryption keys. The proposed algorithm's effectiveness has been substantiated through various analyses, including histogram, correlation, entropy, NPCR and UACI, and noise attack analyses for image and voice encryption. Further research potential lies in developing encryption methods for videos or other complex subjects.

Acknowledgment

The authors express their gratitude for the financial support provided by LP2M UIN Sunan Gunung Djati Bandung and DIKTIS Indonesian Ministry of Religious Affairs (Kementerian Agama Republik Indonesia).

References

[1] D. Xu, G. Li, W. Xu and C. Wei. Design of artificial intelligence image encryption algorithm based on hyperchaos. *Ain Shams Engineering Journal* **14** (3) (2023) 101–891.

[2] D. W. Moore and E. A. Spiegel. A thermally excited non-linear oscillator. *Astrophysical Journal* **143** (1966) 871.

[3] W. S. M. Sanjaya, D. Anggraeni, R. Denya and N. Ismail. Numerical simulation bidirectional chaotic synchronization of spiegel-moore circuit and its application for secure communication. *Annual Applied Science and Engineering Conference* **180** (1) (2017) 89–95.

[4] M. Essaid, I. Akharraz, A. Saaidi and E. A. Mouhib. Image encryption scheme based on a new secure variant of hill cipher and 1d chaotic maps. *Journal of Information Security and Applications* **47** (2019) 173–187.

[5] A. Broumandnia. Designing digital image encryption using 2D and 3D reversible modular chaotic maps. *Journal of Information Security and Applications* **47** (2019) 188–198.

[6] H. Liu, A. Kadir, and J. Liu. Color pathological image encryption algorithm using arithmetic over galois field and coupled hyper chaotic system. *Optics and Lasers in Engineering* **122** (2019) 123–133.

[7] S. Vaidyanathan, A. Sambas, M. Mamat and W. S. M. Sanjaya. Analysis, synchronisation and circuit implementation of a novel jerk chaotic system and its application for voice encryption. *International Journal of Modelling, Identification and Control* **28** (2) (2017) 153–166.

[8] K. Rajagopal, S. Kacar, Z. Wei, P. Duraisamy, K. Teweldbrhan and A. Kartikeyan. Dynamical investigation and chaotic associated behaviors of memristor chua's circuit with a non-ideal voltage-controlled memristor and its application to voice encryption. *International Journal of Electronics and Communications* **107** (2019) 183–191.

[9] A. Phabhakar, A. S. Shetty, K. Z. Tabassum, S. Deb and A. Raghumanth. Voice encryption using chaotic signal. *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* **1** (2023) 1364–1369.

[10] A. N. Negou, J. Kengne and D. Tchiotsop. Periodicity, chaos and multiple coexisting attractors in a generalized moore–spiegel system. *Chaos, Solitons and Fractals* **107** (2018) 275–289.

[11] N. Djafri, T. Hamaizia and F. Derouiche. Boundedness and dynamics of a modified discrete chaotic system with rational fraction. *Nonlinear Dynamics and Systems Theory* **21** (1) (2021) 68–75.

[12] A. Sambas, W. S. M. Sanjaya, M. Mamat, N. V. Karadimas and O. Tacha. Numerical simulations in jerk circuit and it's application in a secure communication system. *Recent Advances in Telecommunications and Circuit Design* **1** (2013) 190–196.

[13] F. Yuan, G. Wang, Y. Shen and X. Wang. Coexisting attractors in a memcapacitor-based chaotic oscillator. *Nonlinear Dynamics* **86** (1) (2016) 37–50.

[14] T. Nestor, A. Belazi, B. Abd-El-atty, M. N. Aslam, C. Volos, N. J. D. Dieu and A. A. El-Latif. A new 4d hyperchaotic system with dynamics analysis, synchronization, and application to image encryption. *Symmetry* **14** (2) (2022) 14–15.

[15] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan and N. Iqbal. A novel and efficient 3d multiple images encryption scheme based on chaotic systems and swapping operations. *IEEE Access* **8** (2020) 123536–123555.

[16] S. Mortajez, M. Tahmasbi, J. Zarei and A. Jamshidnezhad. A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images *Informatics in Medicine Unlocked* **20** (2020) 100396.

[17] L. Xu, X. Gou, Z. Li, and J. Li. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers In Engineering* **91** (2017) 41–52.

[18] A. Elghandour, A. Salah and A. Karawia. A New Cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal.* **13** (1) (2022) 4–5.

[19] P. Sathiyamurthi and S. Ramakrishnan. Speech encryption using chaotic shift keying for secured speech communication. *Eurasip Journal on Audio, Speech, and Music Processing* **2017** (1) (2017) 1–11.

[20] L. Xu, K. Kikushima, S. Sato, A. Islam, T. Sato, S. Aramaki, C. Zhang, T. Sakamoto, F. Eto, Y. Takahashi, I. Yao, M. Machida, T. Kahyo and M. Setou. Spatial distribution of the shannon entropy for mass spectrometry imaging. *PLOS ONE* **18** (4) (2023) 129–177.