An image encryption based on Fibonacci sequence and fusion of advanced encryption standard-least significant bit method

Purwanto[1], Aris Marjuni[1], Erna Zuni Astuti[1], Christy Atika Sari[1], Nova Rijati[1], Pulung Nurtantio Andono[1], Md Kamruzzaman Sarker[2]
[1]Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Department of Computer Science, Bowie State University, Bowie, United States

Article Info

Article history:

Received Feb 15, 2024
Revised Jun 11, 2024
Accepted Aug 30, 2024

Keywords:

Advanced encryption standard
Cryptography
Fibonacci
Image encryption
Least significant bit

ABSTRACT

Image encryption is a vital field ensuring the secure transmission of digital images. In this study, encryption is the core process, employing complex mathematical algorithms and cryptographic keys to transform the original image into a secure format, shielding visual data from unauthorized access during transmission. To enhance security, the research integrates Fibonacci and advanced encryption standard (AES)–least significant bit (LSB) methodologies for a complex key generation system. This mechanism introduces intricate transformations within the image data, creating patterns challenging for potential attackers to decipher. Evaluation of the algorithm's performance reveals efficiency in terms of mean squared error (MSE) and peak signal-to-noise ratio (PSNR). The RGB cover image achieves the lowest MSE of 0.0001 and the highest PSNR values ranging from 44.31 to 49.27. Integration of the Fibonacci sequence notably improves visual quality, enhancing both MSE and PSNR metrics. Unified average changing intensity (UACI) and normalized pixel change rate (NPCR) assessments consistently show the effectiveness of the algorithm, with the RGB cover image presenting the highest UACI and NPCR values. Future research directions involve exploring advanced encryption algorithms, optimizing techniques for high-dimensional datasets, and addressing ethical implications in image encryption, contributing to the development of adaptable and secure solutions.

Corresponding Author:

Aris Marjuni
Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro
Semarang, Indonesia
Email: aris.marjuni@dsn.dinus.ac.id

1. INTRODUCTION

Image cryptography is a sophisticated method that involves the application of cryptographic techniques to ensure the secure transmission of digital images [1], [2]. In image cryptography, encryption is the pivotal process that transforms the original image into an unintelligible and secure format, using complex mathematical algorithms and cryptographic keys [3]. This encrypted version of the image serves as a shield against unauthorized access, interception, or tampering during data transmission, thereby safeguarding the confidentiality and integrity of the visual information [4]. The encryption process involves the utilization of cryptographic keys that significantly influence the pixel values of the image, rendering it indiscernible to the human eye [5], [6]. Cryptographic keys in the encryption phase, the image undergoes a complex transformation that alters the pixel values based on intricate mathematical operations [7], [8]. As a result, the visual representation of the encrypted image appears as seemingly random and meaningless patterns, making it virtually impossible for unauthorized individuals to decipher or perceive the original content without the corresponding decryption keys. This crucial aspect of key-based encryption underscores the crucial role of cryptographic keys in ensuring the imperceptibility and security of the encrypted image data, thereby fortifying the overall integrity of the image cryptography process.

Based on these problems, there is a research objective to enhance the security and imperceptibility of image cryptography through the incorporation of a complex key generation system, using the proposed fusion of Fibonacci advanced encryption standard (AES)-least significant bit (LSB) [9]-[15]. Based on the key generation mechanism, the cryptographic process generates highly convoluted transformations within the image data, resulting in intricate patterns that are exceedingly challenging for potential attackers to decipher [16]. Fibonacci sequence alongside the AES-LSB methodology enhances the complexity of the encryption process, thereby augmenting the overall robustness of the cryptographic system [15], [17]. This advanced amalgamation of cryptographic techniques aims to fortify the security measures against potential breaches or unauthorized access, ensuring that the encrypted image data remains highly resilient and impervious to sophisticated hacking attempts, thus reinforcing the efficacy of the proposed image cryptography framework [18]-[20]. Based on the literature, methodology, and results, this research aims to achieve several objectives and make corresponding contributions. Firstly, it seeks to enhance the robustness and imperceptibility of image cryptography by integrating the Fibonacci AES-LSB technique. Secondly, the effectiveness of the proposed cryptographic framework in securing digital image transmission and storage against potential cyber threats and unauthorized access will be evaluated. Lastly, the research will analyze the performance and resilience of the implemented cryptographic system through comprehensive experimentation and data analysis, thereby establishing its practical viability and applicability in real-world scenarios.

This advanced approach to image cryptography is expected to be further elucidated in subsequent chapters and sub-sections of the research. Section 2 will delve into a comprehensive literature review, examining existing cryptographic methodologies and their applications in image security. Section 3 will expound on the intricate methodology involving the Fibonacci AES-LSB fusion and its implications for image encryption. Subsequently, section 4 will present the detailed results and discussions derived from the implementation of the proposed cryptographic framework, emphasizing its efficacy in enhancing image security and imperceptibility. Finally, section 5 will encapsulate the research findings, providing a comprehensive analysis of the strengths and limitations of the proposed system, along with recommendations for future enhancements and potential applications in broader data security domains.

2. LITERATURE REVIEW

Integration of the Fibonacci sequence in conjunction with established cryptographic techniques, such as AES and LSB encryption, represents a novel approach to image encryption [15], [21], [22]. The Fibonacci sequence introduces a unique dimension to this domain, offering a promising avenue to enhance the security of image encryption systems. This literature review explores the theoretical foundations, applications, and current research landscape surrounding the integration of the Fibonacci sequence with AES and LSB, shedding light on the potential advancements and challenges in this innovative realm of image encryption. Given its acknowledged effectiveness and groundbreaking nature, this approach has undergone continuous development. Research by Sari *et al.* [21], represents a comprehensive investigation into the security aspects of exchanging confidential information over the internet. Their study employs cryptography and steganography techniques, specifically utilizing the Vigenere cipher as a cryptographic method and the LSB technique as a steganographic method. Notably, the research extends its focus to assess the impact of incorporating the Fibonacci sequence into the encryption process. The application of the Fibonacci series in generating a random key for the playfair encryption algorithm introduces an additional layer of complexity to the security framework. Six diverse images, varying in extension, size, and type, serve as the experimental subjects. Research by Maiti *et al.* [22], explores the utilization of Fibonacci transformation and Tribonacci transformation in image encryption, deviating from traditional methods. This technique involves confusing the plain image through Fibonacci transformation and modifying pixel values with Tribonacci transformation. Notably, the Fibonacci and Tribonacci numbers are determined using the hash value of the plain image, marking the first instance of the Tribonacci transformation's application in image encryption. The method demonstrates high key space and sensitivity to the plain image, as observed in evaluations against standard and special images. Furthermore, the research evaluates the proposed method's resistance to various attacks, such as brute force, statistical, differential, noise, cropping, and known/chosen-plaintext attacks. The obtained results highlight the method's resilience and efficiency, comparable to state-of-the-art techniques, emphasizing the advantages brought about by integrating Fibonacci and Tribonacci transformations in image encryption. Research by Guo *et al.* [23], represents a significant stride in addressing the limitations of existing bit scrambling encryption algorithms, specifically their lack of sensitivity to bit scrambling between 8 bits of one pixel and their weakened resistance against noise and selective plaintext attacks. Guo's proposed 3D cyclic shift bit scrambling image encryption algorithm discards the conventional 8-bit pixel scrambling mode and redefines the pixel values by converting them into binary arrays and subsequently into 3D matrices. This novel approach involves the independent scrambling of higher and lower bit-planes, each containing plaintext information of varying weights, through cyclic shifting. The result is an enhanced sensitivity to bit scrambling, improved anti-noise attack capabilities, and increased randomness in the intermediate ciphertext. Notably, Guo introduces a logistic-Fibonacci (L-F) cascade chaos to generate random sequences, mitigating issues associated with blank windows in the uneven distribution of logistic chaos. The last research based on Fibonacci in related research by Anandkumar and Kalpana [24], represents a significant advancement in the domain of digital image encryption, particularly in the utilization of Fibonacci p-code traversing and unified chaotic map-based image encryption (FPT-UCM-IE) scheme. The distinguishing strength of this approach lies in its strategic integration of the Fibonacci sequence, which contributes to three crucial processes: key stream generation, three-iterations-based scrambling, and a single-round diffusion process. Anandkumar's methodology initiates the key generation process through a unified chaotic map, leveraging the chaotic features of the system. Subsequently, the application of Fibonacci p-code Traversing enhances the scrambling process, ensuring a predominant exchange of pixel rows and columns. This distinct approach, coupled with a single-round diffusion process, effectively mitigates strong correlations and simultaneously modifies pixel values between neighboring pixels.

The comprehensive examination of related research in the domain of cryptographic methodologies reveals a prevalent trend toward the incorporation of Fibonacci and Fibonacci sequences. This study specifically focuses on the fusion of the Fibonacci method with established cryptographic techniques, namely AES and LSB steganography. The amalgamation of these methods is undertaken to enhance the overall performance of image encryption systems. The evaluation of this hybridized approach is contingent upon a set of performance metrics, including but not limited to peak signal-to-noise ratio (PSNR), mean squared error (MSE), and other pertinent indicators. Such as, in [2], [3], [6]-[8], [15], [19], [21]-[24].

3. METHOD

In the depicted workflow, the encryption process unfolds through a systematic application of the Fibonacci sequence in conjunction with the amalgamation of AES and LSB methodologies. The secret key "HELLO" initiates the encryption journey, serving as the basis for generating subsequent round keys. The plain image in RGB format undergoes a series of AES operations, including AddRoundKey, SubBytes, ShiftRows, and mix all columns, iteratively repeated over nine rounds. Following this, the application of the Fibonacci sequence comes into play, enhancing the encryption robustness. The subsequent integration of LSB further fortifies the security of the process, especially evident in the grayscale transformation of the plain image. The resultant cipher image in both RGB and grayscale formats showcases the culmination of the Fibonacci-AES-LSB hybrid methodology, as illustrated in Figure 1. The implementation based on the proposed scheme can be seen in the Algorithm 1.

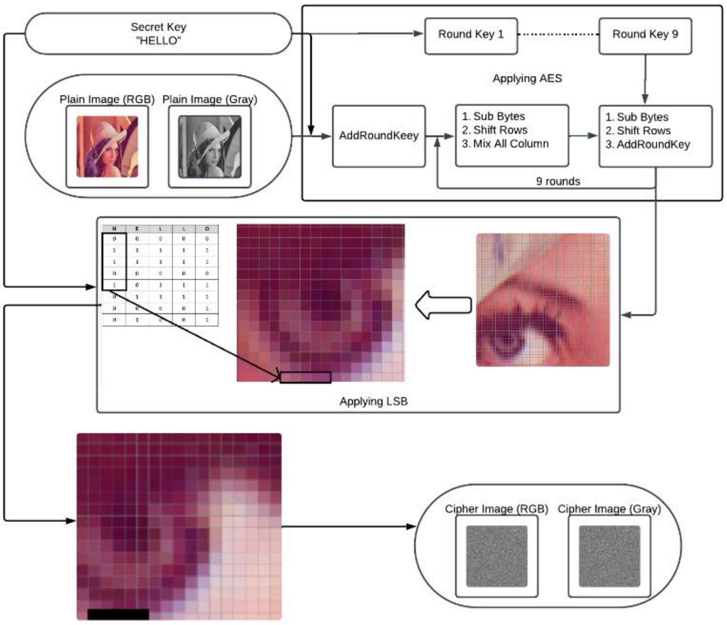


Figure 1. Encryption proposed scheme

3.1. Fibonacci

Fibonacci in image encryption refers to the utilization of the Fibonacci sequence in cryptographic processes to enhance the security of image data [15], [23]. The Fibonacci sequence is a series of numbers in which each number is the sum of the two preceding ones, usually starting with $a = 0$ and $b = 1$ [21]. In the context of image encryption, the Fibonacci sequence is often employed as a key generation mechanism or as a component in the encryption algorithm. Based on the Fibonacci equation can be seen in (1)–(3).

$$F(n) = F(n-1) + F(n-2) \tag{1}$$

with the initial conditions:

$$F(a) = 0, F(b) = 1 \tag{2}$$

This means that the $n - th$ term in the Fibonacci sequence is the sum of the two preceding terms. The Fibonacci sequence starts with 0 and 1, and each subsequent term is calculated by adding the two previous terms. Examples of some terms in the Fibonacci sequence include $0, 1, 1, 2, 3, 5, 8, 13, 21$. Implementation based on the Fibonacci scheme can be seen in Algorithm 2. From (3), the derivatives are obtained as shown in (4) to (6).

Algorithm 1. Encryption proposed scheme

```
Function $Encrypt\_Fibonacci\_AES\_LSB(plain\_image\_rgb, secret\_key)$:
    $initialize\_round\_keys(secret\_key)$
#Generating round keys from the secret key
    for each pixel block in plain_image_rgb:
        # AES Process
        state = $AddRoundKey(pixel\_block, round\_key[0])$
        for $i$ in $range(1, 9)$:
            state = $SubBytes(state)$
            state = $ShiftRows(state)$
            state = $MixColumns(state)$
            state = $AddRoundKey(state, round\_key[i])$
        end
        #Fibonacci Process
        state = $FibonacciEncryption(state)$
        #LSB Process
        state = $ApplyLSB(state)$
        #Final encrypted pixel block
         $cipher\_image\_rgb.append(state)$
return $cipher\_image\_rgb$
```

Algorithm 2. Fibonacci scheme

```
Function $FibonacciEncryption(state)$:
    for each pixel value in the state:
        # Encryption process using Fibonacci sequence
            $pixel\_valuei = pixel\_valuei \oplus FibonacciSequence[i]$    (3)
            $\frac{\partial}{\partial_{xi}} = (pixel\_valuei \oplus FibonacciSequence[i]) = 0$    (4)
            $\frac{\partial}{\partial_{yi}} = (pixel\_valuei \oplus FibonacciSequence[i]) = 0$    (5)
            $\frac{\partial}{\partial_{pixel\_valuei}} = (pixel\_valuei \oplus FibonacciSequence[i]) = 0$    (6)
return $state$
```

3.2. Advanced encryption standard

AES is a widely used symmetric encryption algorithm that is recognized for its strength and efficiency in providing confidentiality and security for sensitive data [25], [26]. In the context of image encryption, AES operates on blocks of data, typically 128 bits in size. Each block undergoes a series of well-defined encryption steps, including substitution (SubBytes), permutation (ShiftRows), mixing of columns (MixColumns), and the addition of a round key (AddRoundKey) [27]. These steps are repeated over multiple rounds to enhance the security of the encryption process. Implementation based on the AES scheme can be seen in the Algorithm 3.

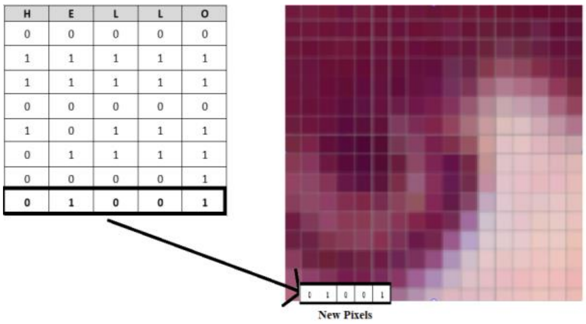
Algorithm 3. AES scheme

```
state = $AddRoundKey(pixel\_block, round\_key[0])$
    for $i$ in range(1,9):
        state = $SubBytes(state)$
            $State_{i,j} = S - Box(State_{i,j})$    (7)
        state = $ShiftRows(state)$
            $State_{i,j} = State_{i(i+j)}\ mod\ 4$          (8)
        state = $MixColumns(state)$
            $State_{i,j} = MixColumn\ (State_{(0,j)} + State_{(1,j)} + \cdots + n)$          (9)
        state = $AddRoundKey(state, round\_key[i])$
            $State_{i,j} = State_{i,j} \oplus round\_key_{i,j}$          (10)
    End
```

3.3. Least significant bit

LSB image encryption is a technique used to hide information within the LSB of the pixel values in an image [14], [28]. The LSB is the binary digit at the far right of a binary representation, and it has the least impact on the overall value of the pixel. LSB image encryption typically involves substituting these LSB with the secret data to be hidden, thereby altering the pixel values in a way that is visually imperceptible to the human eye. Implementation based on the LSB scheme can be seen in Algorithm 4. The insertion process is carried out using the last binary digit from Figure 2. In this process, the last binary digit of each character (H, E, L, L, O) is utilized to embed information into an image or other data. This is achieved by replacing the last binary digit of each pixel in the image with the corresponding bit from Figure 2.

```
Algorithm 4. LSB scheme
Function $ApplyLSB(state)$:
    for each $pixel\_value$ in $state$:
        # LSB application process
        $pixel\_value =$
$(pixel\_value\ \&\ 0b11111110)\ |\ LSBData$
return $state$
```



H	E	L	L	O
0	0	0	0	0
1	1	1	1	1
1	1	1	1	1
0	0	0	0	0
1	0	1	1	1
0	1	1	1	1
0	0	0	0	1
0	1	0	0	1

0	1	0	0	1

Figure 2. Sample bit and LSB concept based on key

3.4. Quality measurement

In this research, the assessment of image quality is conducted through a comprehensive measurement framework comprising MSE, PSNR, normalized pixel change rate (NPCR), and unified average changing intensity (UACI). The quality metrics are formulated as per (11)-(14) [29]. MSE quantifies the average squared difference between the original and encrypted images, indicating reconstruction accuracy. PSNR assesses the fidelity of the encrypted image by comparing it to the original, taking into account the maximum possible pixel value. NPCR gauges the percentage of differing pixels between the original and encrypted images, emphasizing the importance of individual pixel variations. UACI measures the average intensity change in the image, offering insights into the global alterations introduced during the encryption process. The equation based on quality measurement can be seen in (11)–(14):

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I(i,j) - K(i,j)\right)^2 \qquad (11)$$

$$PSNR = 10 \log 10 \left(\frac{\max\_pixel\_value^2}{MSE}\right) \qquad (12)$$

$$NPCR = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left|\frac{I(i,j) - K(i,j)}{I(i,j)}\right| \times 100 \qquad (13)$$

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|\frac{I(i,j) \oplus K(i,j)}{L}\right| \times 100 \qquad (14)$$

4. RESULTS AND DISCUSSION

The research incorporates a diverse set of classical images, namely Lena, Airplane, Baboon, and Peppers, as the cover data for the image encryption evaluation, as illustrated in Figures 3(a) to (d). These images, widely recognized and utilized in image processing studies, offer a comprehensive representation of various visual content, structures, and complexities. Following the selection of datasets, as illustrated in Figures 3(a) to (d) and Figures 4(a) to (d), the research proceeds with the crucial step of initializing the secret key. This key, as described in the Algorithm 5, plays a pivotal role in governing the cryptographic processes applied to the chosen classical images-figure (a) represent Lena, figure (b) represent Airplane, figure (c) represent Baboon, and figure (d) represent Peppers.

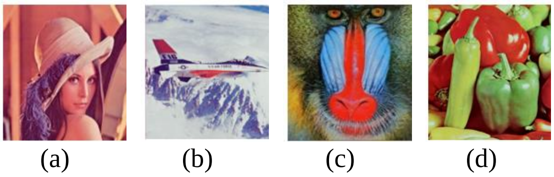


Figure 3. Sample cover datasets (RGB): (a) Lena.png, (b) Airplane.png, (c) Baboon.png, and (d) Peppers.png

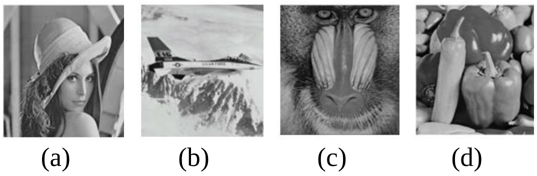


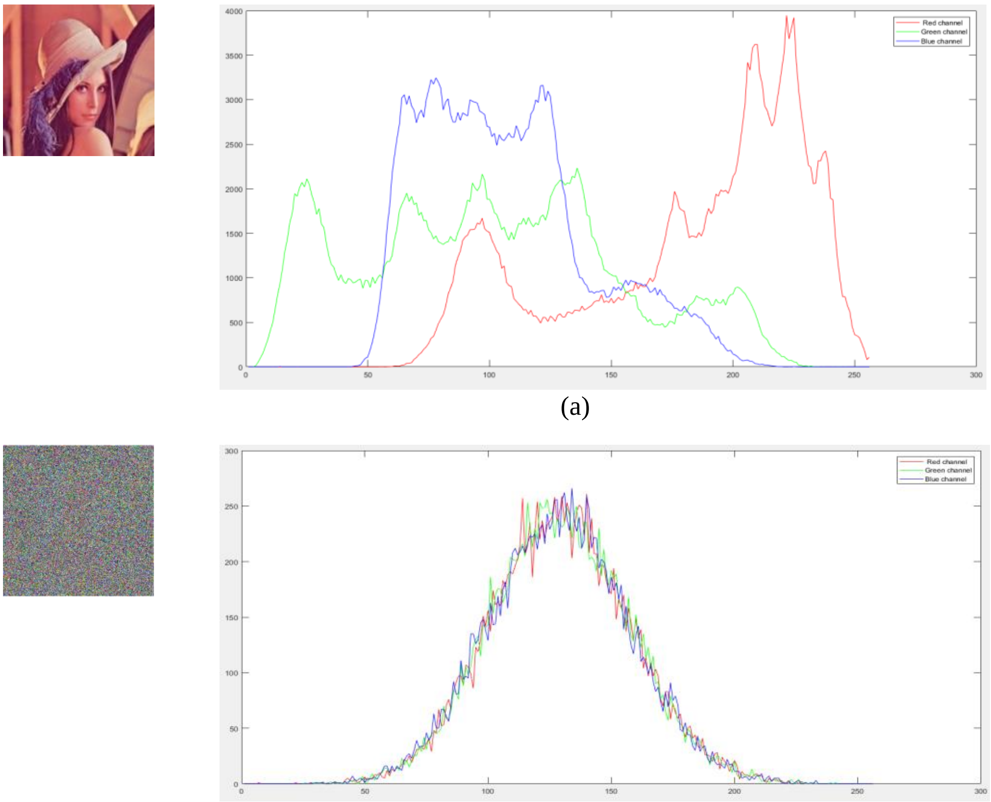
Figure 4. Sample cover datasets (gray): (a) Lena.png, (b) Airplane.png, (c) Baboon.png, and (d) Peppers.png

```
Algorithm 5. Initialize secret key
Procedure $initialize\_round\_keys(secret\_key)$:
    # Key expansion process for generating round keys using AES method
    $round\_key[0] = secret\_key$
    for $i$ in range$(1, 10)$:
        $round\_key[i] = KeyExpansion(round\_key[i-1], i)$
    end
```

In Figure 5(a), the cover RGB image is presented without the use of the Fibonacci sequence, where the transformations are not immediately noticeable, thereby retaining much of the visual content of the original image. However, in Figure 5(b), the corresponding encrypted image becomes visibly distorted, showcasing the encryption algorithm’s effectiveness in concealing the original information. Similarly, in Figure 6(a), the grayscale cover image is displayed, also without the incorporation of the Fibonacci sequence, maintaining a visual similarity to the original. Yet, in Figure 6(b), the encrypted grayscale image exhibits significant distortion, further emphasizing the algorithm’s strength in securing both RGB and grayscale images.

However, in Figures 7(a) and (b), a subsequent phase involved the embedding of the Fibonacci sequence. This additional step led to a remarkable enhancement in the visual quality of the encrypted image, rendering it closely resembling the original. Figure 7(a) presents the original RGB image after the incorporation of the Fibonacci sequence, based on the original cover image. The integration of the Fibonacci sequence significantly enhances the visual quality, resulting in an encrypted image that closely resembles the original. Subsequently, Figure 7(b) displays the encrypted image, further emphasizing the improvement brought by the Fibonacci sequence, which plays a pivotal role in refining both the perceptual quality and the effectiveness of the encryption algorithm. Similarly, Figure 8(a) illustrates the original grayscale image based on the cover image with the Fibonacci sequence applied, demonstrating a substantial improvement in visual similarity to the original. Figure 8(b) then shows the final encrypted grayscale image, where the enhancement in clarity and quality is evident, further reinforcing the critical impact of the Fibonacci sequence in optimizing the perceptual quality of encrypted images across both RGB and grayscale formats.

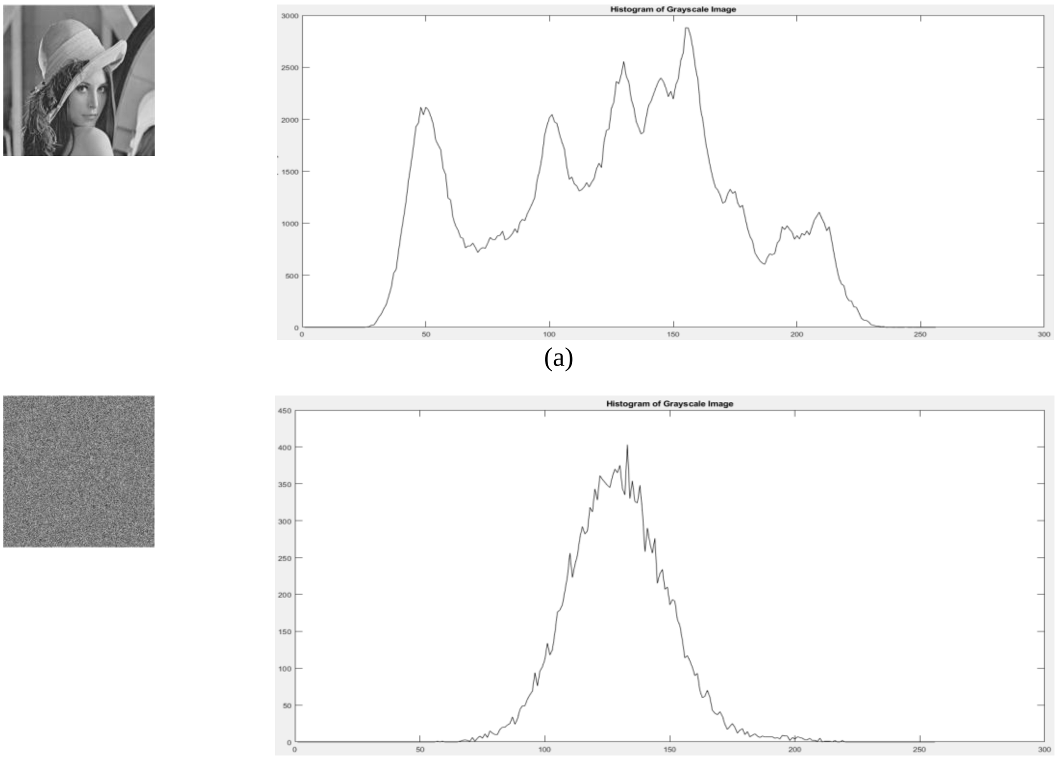
The utilization of the Fibonacci sequence in the encryption process for Figures 7(b) and 8(b) has yielded notable outcomes, as reflected in the MSE and Peak PSNR values meticulously recorded in Table 1. The incorporation of the Fibonacci sequence has proven instrumental in refining the visual quality of the encrypted images, with Figure 7(b) showcasing a significant improvement compared to its non-Fibonacci counterpart in Figure 5(b). Following the meticulous measurement of MSE and PSNR, the subsequent phase involved the comprehensive evaluation of UACI and NPCR, as detailed in Tables 2 and 3.



(a)

(b)

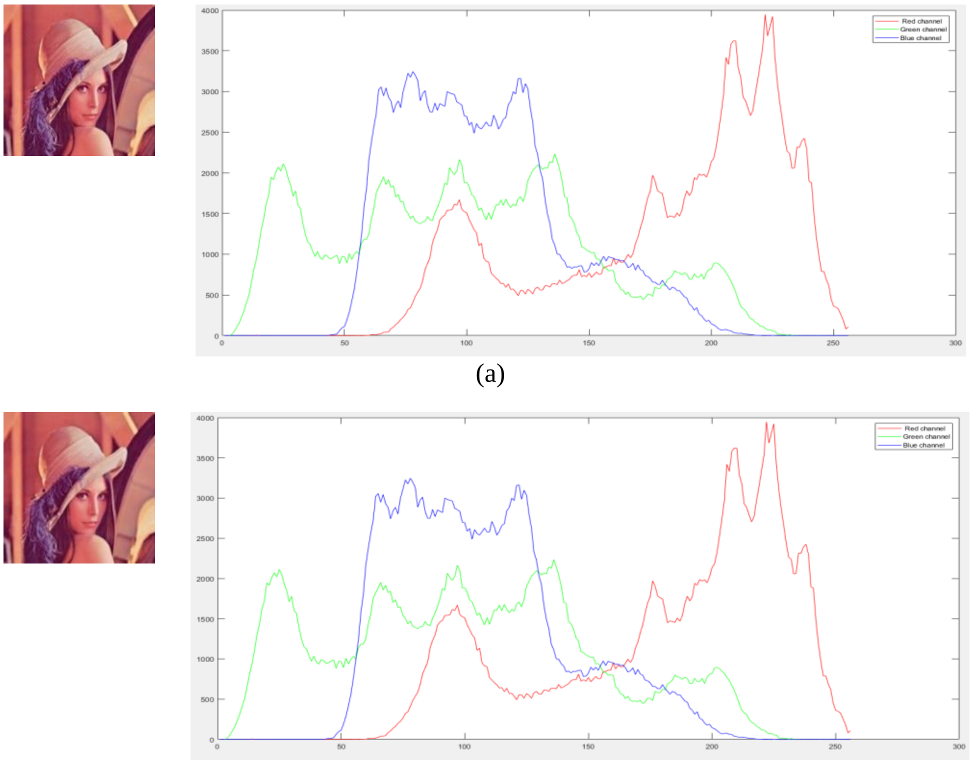
Figure 5. Encrypted image and histogram image (RGB) without Fibonacci: (a) based on cover image and (b) based on encrypted image



(a)

(b)

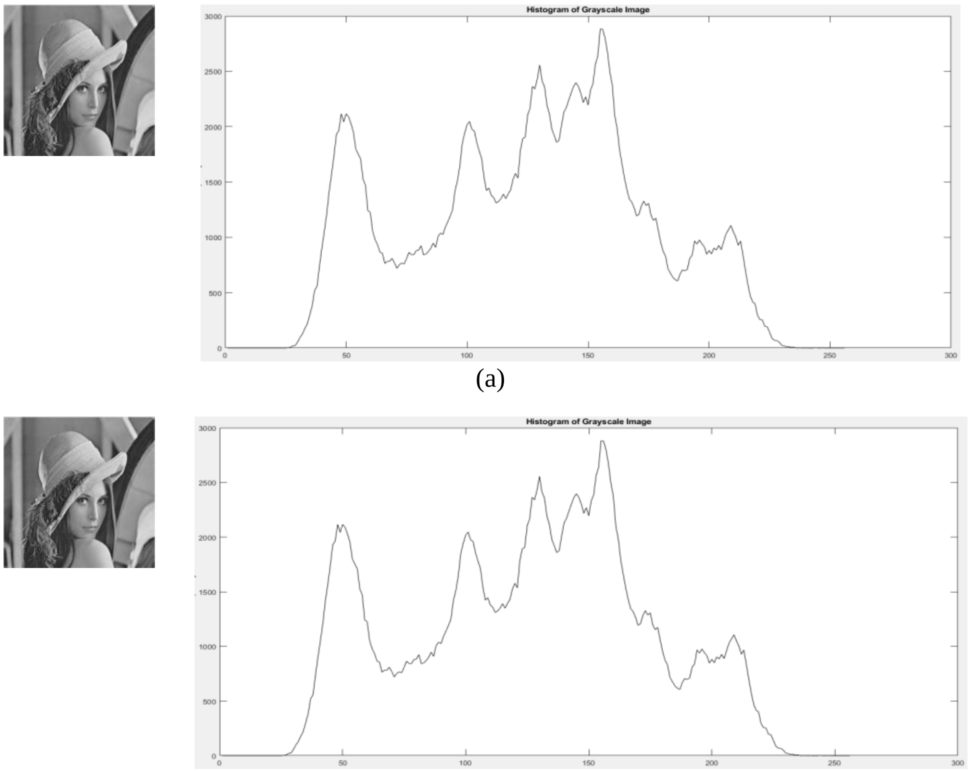
Figure 6. Encrypted image and histogram image (gray) without Fibonacci: (a) based on cover image and (b) based on encrypted image



(a)

(b)

Figure 7. Encrypted image and histogram image (RGB) with Fibonacci: (a) based on cover image and (b) based on encrypted image



(a)

(b)

Figure 8. Encrypted image and histogram image (gray) with Fibonacci: (a) based on cover image and (b) based on encrypted image

Table 1. Quality measurement based on MSE and PSNR between original image and encrypted image

MSE/PSNR	Cover image	Research	Lena	Airplane	Baboon	Peppers
MSE	RGB	Our research	0.0001	0.0003	0.0001	0.0002
	Grayscale		0.0001	0.0003	0.0001	0.0001
	RGB	[21]	0.0001	-	-	-
	RGB	[30]	0.01804	-	0.01253	0.02556
	RGB	Our research	90 dB	82 dB	91 dB	92 dB
	Grayscale		99 dB	96 dB	99 dB	99 dB
PSNR	RGB	[21]	88 dB	-	-	-
	RGB	[30]	65.6 dB	-	67.2 dB	64.1 dB

Table 2. Quality measurement based on UACI

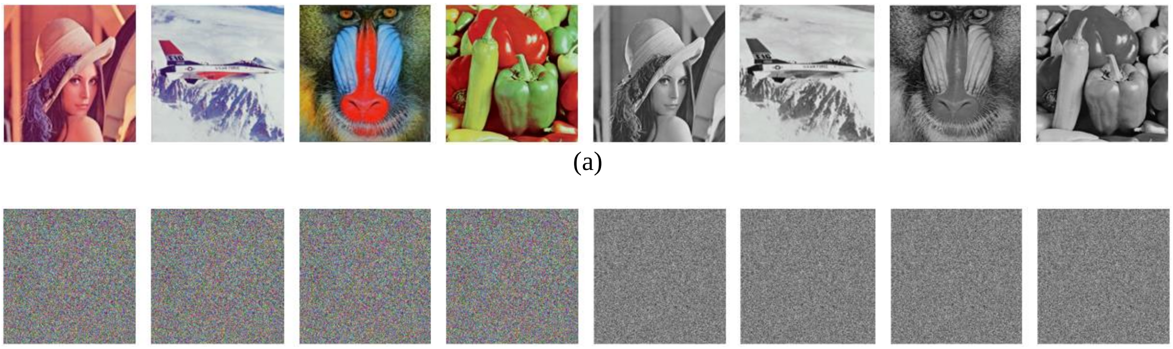
Cover image	Research	Lena	Airplane	Baboon	Peppers
RGB	Our research	49.19	44.31	49.27	48.13
Grayscale		49.19	44.31	49.27	48.13
RGB	[21]	49.002	-	-	-
RGB	[22]	33.45	-	33.47	33.43
RGB	[23]	33.51	-	33.53	-
Grayscale		33.48	-	33.43	-
RGB	[24]	33.21	-	33.45	-

Table 3. Quality measurement based on NPCR

Cover image	Research	Lena	Airplane	Baboon	Peppers
RGB	Our research	49.19	44.31	49.27	48.13
Grayscale		49.19	44.31	49.27	48.13
RGB	[21]	99.88	-	-	-
RGB	[22]	99.61	-	99.60	99.62
RGB	[23]	99.61	-	99.61	-
Grayscale		99.61	-	99.59	-
RGB	[24]	99.72 (Highest)	-	99.82 (Highest)	-

In the histograms displayed for each image, the horizontal axis represents the intensity values of the pixels, ranging from 0 to 255 for grayscale images, where 0 corresponds to pure black and 255 corresponds to pure white. In the case of color images, the histogram is typically generated for each color channel (red, green, and blue). The vertical axis, on the other hand, denotes the frequency or the number of pixels that possess a particular intensity value. Thus, a higher bar in the histogram indicates a greater number of pixels in the image that share the same intensity level, providing valuable insights into the distribution of pixel intensities within the analyzed image.

Figures 9(a) and (b) depicts a compelling visual representation of the encrypted image, showcasing the discernible impact of incorporating the Fibonacci sequence into the encryption process. The side-by-side comparison contrasts the encrypted image with and without the application of the Fibonacci sequence. In the version without Fibonacci, the encrypted image exhibits a certain level of obscurity, with visual details being notably challenging to decipher.



(a)

(b)

Figure 9. Encrypted image results: (a) with Fibonacci and (b) without Fibonacci

5. CONCLUSION

In conclusion, the meticulous evaluation of the image encryption algorithm's performance reveals compelling insights. The analysis based on MSE and PSNR demonstrated the algorithm's efficiency, with the RGB cover image achieving the lowest MSE of 0.0001 and the highest PSNR values ranging from 44.31 to 49.27. Furthermore, the integration of the Fibonacci sequence notably improved the visual quality of the encrypted images, leading to a substantial enhancement in both the MSE and PSNR metrics. Moving on to the evaluation based on UACI, the RGB cover image consistently exhibited the highest UACI values across all research images, ranging from 44.31 to 49.27. Similarly, the assessment utilizing the NPCR further reinforced the algorithm's effectiveness, with the RGB cover image consistently presenting the highest NPCR values, indicating lower pixel changes between the original and encrypted images. These findings collectively underscore the algorithm's robustness in preserving image integrity and quality, with the RGB cover image consistently outperforming the grayscale counterpart. In future research, exploring advanced encryption algorithms, including machine learning-based approaches, could open new avenues for secure image transmission and storage. Optimizing encryption techniques for handling high-dimensional and large-scale image datasets is crucial, given the evolving landscape of imaging technologies. Additionally, investigating the resilience of image encryption against emerging threats, especially quantum computing attacks, is essential for ensuring long-term security. Real-world applications, such as secure multimedia communication and medical image confidentiality, provide fertile ground for assessing the usability and performance of encryption algorithms. Addressing the ethical implications of image encryption is equally important, fostering the development of frameworks that balance privacy, security, and responsible deployment. These future research directions aim to contribute to the advancement of robust and adaptable image encryption solutions in diverse contexts.

ACKNOWLEDGEMENTS

The author would like to thank the Research Center for Intelligent Distributed Surveillance and Security which has provided support in the form of discussion space, laboratory, and funding for this research.

REFERENCES

[1] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[2] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, P. Kumaresan, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–19, Sep. 2020, doi: 10.3390/s20185162.

[3] P. Manisekaran, P. Dhankhar, and P. Kumar, "Approaches of Chaotic Image Encryption models in Enlightening Image Storage and Security systems," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 2, pp. 997–1005, Apr. 2021, doi: 10.30534/ijatcse/2021/731022021.

[4] V. Sathananthavathi, K. G. Kumar, and M. S. Kumar, "Secure visual communication with advanced cryptographic and ımage processing techniques," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 45367–45389, Oct. 2024, doi: 10.1007/s11042-023-17224-6.

[5] Y. G. Yang, F. E. Cheng, D. H. Jiang, Y. H. Zhou, W. M. Shi, and X. Liao, "A visually meaningful image encryption algorithm based on P-tensor product compressive sensing and newly-designed 2D memristive chaotic map," *Physica Scripta*, vol. 98, no. 10, p. 105211, Oct. 2023, doi: 10.1088/1402-4896/acf52d.

[6] M. Roy, S. Chakraborty, and K. Mali, "An optimized image encryption framework with chaos theory and EMO approach," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 30309–30343, Aug. 2023, doi: 10.1007/s11042-023-14438-6.

[7] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation," *Visual Computer*, vol. 38, no. 3, pp. 1027–1050, Mar. 2022, doi: 10.1007/s00371-021-02066-w.

[8] S. Patel, K. P. Bharath, and R. Kumar, "Symmetric keys image encryption and decryption using 3D chaotic maps with DNA encoding technique," *Multimedia Tools and Applications*, vol. 79, no. 43–44, pp. 31739–31757, Nov. 2020, doi: 10.1007/s11042-020-09551-9.

[9] J. G. Edwar and M. A. Holman, "Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, 2022, doi: 10.14569/ijacsa.2022.01308104.

[10] S. R. Mohamed, M. Kabeer, N. Rajendran, and I. S. Ali, "Enhanced Security in Supply Chain Management System Using AES and Md5 Algorithms," *Journal of Pharmaceutical Negative Results*, vol. 13, no. SO3, pp. 78–84, Jan. 2022, doi: 10.47750/pnr.2022.13.s03.014.

[11] Q. S. Alsaffar, H. N. Mohaisen, and F. N. Almashhdini, "An encryption based on DNA and AES algorithms for hiding a compressed text in colored Image," *IOP Conference Series: Materials Science and Engineering*, vol. 1058, no. 1, p. 012048, Feb. 2021, doi: 10.1088/1757-899x/1058/1/012048.

[12] M. Rohini, M. A. Srikanth, M. Prajwal, P. R. Kumar, M. Basavaraj, and M. U. Vinay, "Advanced Data Security Using Modulo Operator And LSB Method," *Journal of Scholastic Engineering Science and Management*, vol. 2023, no. 5, pp. 26–37, 2023, doi: 10.5281/zenodo.7890771ï.

[13] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 3559–3568, Jun. 2022, doi: 10.1016/j.jksuci.2020.12.017.

[14] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A comprehensive review on medical image steganography based on LSB technique

and potential challenges," *Baghdad Science Journal*, vol. 18, pp. 957–974, Jun. 2021, doi: 10.21123/bsj.2021.18.2(Suppl.).0957.

[15] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Computing and Applications*, vol. 34, no. 21, pp. 19313–19341, Nov. 2022, doi: 10.1007/s00521-022-07493-x.

[16] M. Hussain, N. Iqbal, and Z. Bashir, "A chaotic image encryption scheme based on multi-directional confusion and diffusion operations," *Journal of Information Security and Applications*, vol. 70, p. 103347, Nov. 2022, doi: 10.1016/j.jisa.2022.103347.

[17] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, p. 287, Mar. 2023, doi: 10.3390/fractalfract7040287.

[18] A. Jan, S. A. Parah, and B. A. Malik, "IEFHAC: Image encryption framework based on hessenberg transform and chaotic theory for smart health," *Multimedia Tools and Applications*, vol. 81, no. 13, pp. 18829–18853, May 2022, doi: 10.1007/s11042-022-12653-1.

[19] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical Image Encryption: A Comprehensive Review," *Computers*, vol. 12, no. 8, p. 160, Aug. 2023, doi: 10.3390/computers12080160.

[20] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[21] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, Aug. 2023, doi: 10.22266/ijies2023.0831.46.

[22] C. Maiti, B. C. Dhara, S. Umer, and V. Asari, "An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations," *IEEE Access*, vol. 11, pp. 48421–48440, 2023, doi: 10.1109/ACCESS.2023.3276723.

[23] Y. Guo, S. Jing, Y. Zhou, X. Xu, and L. Wei, "An image encryption algorithm based on logistic-fibonacci cascade chaos and 3D bit scrambling," *IEEE Access*, vol. 8, pp. 9896–9912, 2020, doi: 10.1109/ACCESS.2019.2963717.

[24] R. Anandkumar and R. Kalpana, "A Fibonacci p-code traversing and unified chaotic map-based image encryption algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 8, pp. 3713–3727, Aug. 2022, doi: 10.1007/s12652-021-03659-y.

[25] P. Bagane and S. Kotrappa, "Enriching aes through the key generation from genetic algorithm," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 4, pp. 955–963, Aug. 2021, doi: 10.21817/indjcse/2021/v12i4/211204141.

[26] B. Xing, D. D. Wang, Y. Yang, Z. Wei, J. Wu, and C. He, "Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor," *International Journal of Parallel Programming*, vol. 49, no. 3, pp. 463–486, Jun. 2021, doi: 10.1007/s10766-021-00692-4.

[27] M. Kumar, A. Soni, A. R. S. Shekhawat, and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, IEEE, Feb. 2022, pp. 1453–1457, doi: 10.1109/ICAIS53314.2022.9742942.

[28] M. H. Mahdi, A. A. Abdulrazzaq, M. S. Mohd Rahim, M. S. Taha, H. N. Khalid, and S. A. Lafta, "Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption," *IOP Conference Series: Materials Science and Engineering*, vol. 518, no. 5, p. 052002, May 2019, doi: 10.1088/1757-899X/518/5/052002.

[29] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[30] W. Alexan, A. Hamza, and H. Medhat, "An AES Double-Layer Based Message Security Scheme," in *Proceedings of 2019 International Conference on Innovative Trends in Computer Engineering, ITCE 2019*, IEEE, Feb. 2019, pp. 86–91, doi: 10.1109/ITCE.2019.8646461.

BIOGRAPHIES OF AUTHORS

Purwanto is currently an Associate Professor in the Faculty of Computer Science at the University of Dian Nuswantoro, Semarang, Indonesia. He received his Ph.D. degree from the Faculty of Computing and Informatics Multimedia University, Cyberjaya, Malaysia. Now, he serves as Head of the Master's degree Program at the University of Dian Nuswantoro. He has published research papers in reputed international journals and conferences. His current research interests image processing, machine learning, and deep learning. He can be contacted at email: purwanto@dsn.dinus.ac.id.

Aris Marjuni was born in Wonogiri, Jawa Tengah, Indonesia, in 1969. He received a Doctoral degree in Electrical Engineering from Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2019. He is currently an Associate Professor with the Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Jawa Tengah, Indonesia. His research interests include image processing, data mining, software engineering, soft computing, information systems, and statistics. He can be contacted at email: aris.marjuni@dsn.dinus.ac.id.

Erna Zuni Astuti received her Bachelor's degree from the University of Gajah Mada in 1998, and her Master's degree from the University of Dian Nuswantoro in 2006. She is an Associate professor in the Faculty of Computer Science. Since 1997 she has been a lecturer at the University of Dian Nuswantoro. The teaching fields are informatics logic, and statistics which are the basis for developing informatics learning. Her research interests are data security, digital image processing, computational, and artificial intelligence. She can be contacted at email: erna.zuni.astuti@dsn.dinus.ac.id.

Christy Atika Sari received the Master's degree in Informatic Engineering from Dian Nuswantoro University and University Teknikal Malaysia Melaka (UTeM) in 2012. She is currently active as an author in an international journal and conference Scopus indexed. She was also awarded as best author and best paper at a national and international conference in 2019 and 2020 respectively and was awarded by the Indonesian Ministry of Education and Culture Research and Technology as the Indonesian top 50 best researchers in 2020. She's research interest is image processing, data hiding, and deep learning. She can be contacted at email: atika.sari@dsn.dinus.ac.id.

Nova Rijati received a Bachelor's degree from the Mathematics Department, Universitas Diponegoro, Semarang, in 1995, a Master's degree in Informatics Engineering from STTIBI, Jakarta, in 2001, and a Ph.D. degree in Intelligent Electrical and Informatics Technology from Institut Teknologi Sepuluh Nopember, Surabaya, in 2021. She is an IEEE and IAENG member. She is currently with the Informatics Department, Universitas Dian Nuswantoro, Semarang, Jawa Tengah, Indonesia. Her research interests include computer science, artificial intelligence, and data mining. She can be contacted at email: nova.rijati@dsn.dinus.ac.id.

Pulung Nurtantio Andono received a Bachelor's degree from Trisakti University, Jakarta, Indonesia, in 2006, a Master's degree from Dian Nuswantoro University, Semarang, Indonesia, in 2009, and a Ph.D. degree from the Institut Teknologi Sepuluh November (ITS), Surabaya, Indonesia, in 2016. He currently works as a lecturer and a researcher at the Faculty of Computer Science, Dian Nuswantoro University. His research interests include image security, computer vision, and 3D image reconstruction. He has authored or co-authored more than 43 refereed journals and conference papers indexed by Scopus. He can be contacted at email: pulung@dsn.dinus.ac.id.

Md Kamruzzaman Sarker is an Assistant Professor of Computer Science at the Bowie State University. He love to invent new stuff (research), share knowledge (teaching), and at the same time build stuff (software engineering). His research domain spans the broad field of artificial intelligence (AI) and its application. Some specific topics of focus include but are not limited to explainable artificial intelligence, deep learning, knowledge graphs, semantic web, and CyberSecurity. He can be contacted at email: ksarker@bowiestate.edu.