

Strengthening Image Security with Unimodular Hill Cipher and Advanced Encryption Standard

¹Samsul Arifin, ²Dwi Wijonarko, ¹Monica Mayeni Manurung, ¹Roni, ³Puguh Wahyu Prasetyo and ⁴Fabian Surya Pramudya

¹Department of Data Science, Faculty of Engineering and Design, Institut Teknologi Sains Bandung, Bekasi, West Java, Indonesia

²Department of Information Technology, Faculty of Computer Science, University of Jember, Jember, East Java, Indonesia

³Department of Mathematics Education, Faculty of Teacher Training and Education, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

⁴Department of Mathematics, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia

Article history

Received: 21-09-2024

Revised: 24-12-2024

Accepted: 18-1-2025

Corresponding Author:

Samsul Arifin

Department of Data Science,
Faculty of Engineering and
Design, Institut Teknologi
Sains Bandung, Bekasi, West
Java, Indonesia

Email: samsul.arifin@itsb.ac.id

Abstract: Digital data security has become increasingly important with the growth of digital image usage, which often contains sensitive information. This study aims to enhance the security of digital images by combining Unimodular Hill Cipher (UHC) and Advanced Encryption Standard (AES) methods. UHC, a matrix-based symmetric encryption algorithm, is used for image matrix encryption, while AES provides an additional layer of security to protect images against advanced cryptographic attacks. The methodology involves several stages: Preprocessing digital images into matrix form, encrypting matrix blocks using UHC, and applying AES encryption for further protection. The encryption and decryption processes are implemented using Python programming, utilizing libraries such as NumPy, Pillow, and PyCryptodome. Experimental analysis evaluates time efficiency, data integrity, and resistance to cryptographic attacks. The results show that the hybrid UHC-AES method significantly enhances security by randomizing pixel values, as evidenced by entropy analysis, histogram comparison, and correlation evaluation. The entropy values indicate high randomness, and the correlation analysis shows no relationship between the original and encrypted images, ensuring strong encryption. Additionally, the method performs efficiently for medium-sized image files, with encryption times increasing proportionally to key size. Despite its effectiveness, challenges remain, particularly in optimizing the encryption speed for large files and addressing key management vulnerabilities. This study contributes to advancing digital image security by integrating UHC and AES into a robust hybrid cryptographic approach. It opens avenues for future research on developing more efficient algorithms and exploring real-time applications in multimedia data protection.

Keywords: Unimodular Hill Cipher, AES, Digital Image Encryption, Data Security, Python, Cryptography

Introduction

Digital data security has become a top priority in this information age, where the volume of data collected, stored, and shared continues to increase exponentially. One form of data that requires special attention in terms of security is digital images. Digital images often contain sensitive information, such as personal documents, medical records, or confidential company information, so protection against unauthorized access is essential. Cryptographic technology plays a crucial role in protecting digital data, especially in maintaining the

confidentiality, integrity, and authentication of digital images from cyberattacks (Lone and Singh, 2020). Digital images that are not properly protected are vulnerable to threats such as eavesdropping, unauthorized alteration, and illegal distribution. The main challenge in maintaining the confidentiality and integrity of digital images lies in the complexity of adequate encryption without sacrificing efficiency in the storage and transmission process. Therefore, a strong yet efficient encryption method is needed to protect digital images from third-party threats (Arifin *et al.*, 2022; Sreejith and Senthil, 2021).

The reviewed works highlight advancements in cryptographic architectures that address both reliability and performance challenges in securing sensitive communication. First, error detection mechanisms, such as recomputing with encoded operands and signature-based schemes, are proposed to enhance the resilience of lightweight block ciphers against transient and permanent faults, ensuring the simultaneous provision of confidentiality, integrity, and authenticity. Second, the implementation of Supersingular Isogeny Diffie-Hellman (SIDH) on FPGA introduces constant-time hardware optimizations that achieve significant speed improvements in key exchange protocols, leveraging heavily parallelized arithmetic for high-security levels, including quantum-resilient operations. Lastly, a scalable architecture for isogeny-based cryptosystems further improves efficiency with a focus on high-bit quantum security, achieving faster computations and supporting additional cryptographic applications such as digital signatures. Collectively, these works underscore the importance of integrating fault tolerance and high-performance computation in modern cryptographic systems to enhance both security and reliability (Subramanian *et al.*, 2017; Koziel *et al.*, 2016); (Koziel *et al.*, 2018).

Unimodular Hill Cipher is a matrix-based encryption algorithm that belongs to symmetric cryptography, where the same key is used for encryption and decryption processes. In Hill Cipher, keys in the form of invertible matrices are used to convert the original message into an encrypted form. This matrix serves as the encryption key, and for decryption, the inverse matrix of the key is used to return the original message. As a form of block cipher, Unimodular Hill Cipher processes data by dividing it into blocks that are then encrypted using a key matrix. This is like other symmetric algorithms such as AES, which also work on fixed-size blocks of data. Due to its simple and efficient nature, Hill Cipher provides good speed in the encryption and decryption process, making it suitable for applications that require high performance. However, like other symmetry methods, Hill Cipher is vulnerable to attacks if the key or matrix pattern is guessable or if too much data is encrypted without a key change. Therefore, while effective in certain situations, Hill Cipher is often combined with stronger symmetric encryption algorithms such as AES to enhance security and protect data from more sophisticated cryptographic threats (Arifin *et al.*, 2021; 2024). This is stated in the following Fig. (1), which illustrates a comparison between symmetric encryption and asymmetric encryption methods.

In symmetric encryption, the same secret key is used for both encryption and decryption processes. Data in plaintext form is converted into ciphertext using the secret key, and the ciphertext can be reverted back to plaintext using the same key. This method is

faster and computationally efficient, making it ideal for protecting large amounts of data. However, the main challenge lies in securely sharing the key with authorized parties without risking its exposure. On the other hand, asymmetric encryption uses two different keys: A public key for encryption and a private key for decryption. Data encrypted with the public key can only be decrypted by its corresponding private key. This method is more secure since the private key is never shared. However, asymmetric encryption tends to be slower due to higher computational requirements. It is often used for key exchange and authentication in security systems. Modern systems frequently combine these two methods to leverage the speed of symmetric encryption and the security of asymmetric encryption (Awati *et al.*, 2024).

Here is a comparison with some of our previous works, where this study aims to refine all the processes from before. This research discusses the use of the Hill Cipher in digital image encryption by combining several techniques, including unimodular matrices and the logistic map. In this method, the unimodular matrix, which has an inverse, is used as the encryption key, while the logistic map is used to generate the encryption keys. The encryption process is carried out by matrix multiplication modulo and can be enhanced with Shift Cipher 128 to handle incomplete parts of the file. This algorithm improves security by adding encryption layers, and experimental results show that it provides very secure encryption with faster encryption times than other algorithms. Thus, this approach holds promise for digital image encryption applications that require high security and fast processing times (Arifin *et al.*, 2022; 2023; Muktyas *et al.*, 2021).

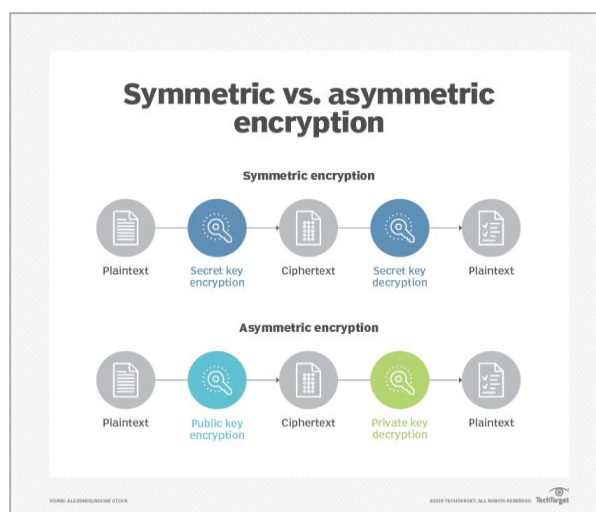


Fig. 1: Symmetric and asymmetric encryption concepts (Awati *et al.*, 2024)

Advanced Encryption Standard (AES) is a symmetric block encryption algorithm chosen by the US government to protect confidential information. AES is widely applied worldwide in software and hardware to encrypt sensitive data. This encryption method is crucial in government computer security, cybersecurity, and electronic data protection. By dividing messages into small 128-bit blocks and running multiple rounds of encryption, AES offers stronger and more reliable security than previous methods of symmetric encryption. AES uses keys with a length of 128, 192, or 256 bits to encrypt and decrypt data, ensuring the confidentiality and integrity of information. As a symmetrical algorithm, AES uses the same key for the encryption and decryption process, so the sender and receiver must have the same secret key. The cipher block used in AES ensures that every part of the plaintext message is converted into an incomprehensible ciphertext without a decryption key. Larger key lengths are used to protect high-level confidential information, such as government or military data, although it requires more processing power. AES was officially adopted by the National Institute of Standards and Technology (NIST) (2003) as a standard encryption algorithm for protecting confidential information, including government information. It is also the first open password approved by the National Security Agency to protect Top Secret information. AES is currently widely used in a variety of commercial and government encryption applications, including storage media, electronic communications, wireless networks, databases, VPNs, and more, making it one of the most popular symmetric key cryptographic algorithms in the world (Hussein and Amintoosi, 2023; Chowdhary *et al.*, 2020). This is stated in the following Fig. (2).

This study aims to apply a combination of Unimodular Hill Cipher and Advanced Encryption Standard (AES) methods for digital image encryption. Both methods will be implemented using the Python programming language, with the hope of producing a secure and efficient encryption solution to protect digital images from various cryptographic attacks. Unimodular Hill Cipher is a variant of the classic Hill Cipher, which uses an unimodular matrix (The Determinant is ± 1) to encrypt data. This method involves the use of linear algebra, where a key matrix is used to perform a linear transformation on a block of data, in this case, a digital image pixel, thus producing a ciphertext. Encryption keys can be easily inverted due to their unimodular nature, so the decryption process can be carried out efficiently. AES is one of the most

widely used encryption algorithms and is considered a modern encryption standard. AES uses a symmetrical cipher block with a block size of 128 bits and a variable key length (128, 192, or 256 bits). AES is well-known for its ability to provide a high level of security with relatively fast processing times, so it is widely adopted to protect digital data in a variety of applications, including image encryption (Lone and Singh, 2020; Lone *et al.*, 2022; Azanuddin *et al.*, 2024).

Digital image encryption is a technique that converts the original representation of an image into an unrecognizable form, thus ensuring that only authorized authorities can access the original image. This process involves transforming image data using various cryptographic algorithms. The image encryption method can include transforming a pixel or block of pixels into ciphertext, which can then be re-described by the receiver who has the decryption key. Several studies have shown the effectiveness of encryption methods in protecting digital images. For example, research on the use of AES and other matrix-based methods shows that cryptography can improve the security of image data without sacrificing quality or file size. A combination of more complex methods, such as combining Hill Cipher with AES, is expected to provide a higher level of security than using a single method alone (Suryadi *et al.*, 2021; Sharma *et al.*, 2022). Table (1) compares the strengths and weaknesses of the Unimodular Hill Cipher (UHC) and the Advanced Encryption Standard (AES) algorithms (Arifin *et al.*, 2022; 2021; 2024; Muktyas *et al.*, 2021; National Institute of Standards and Technology (US). (2023).

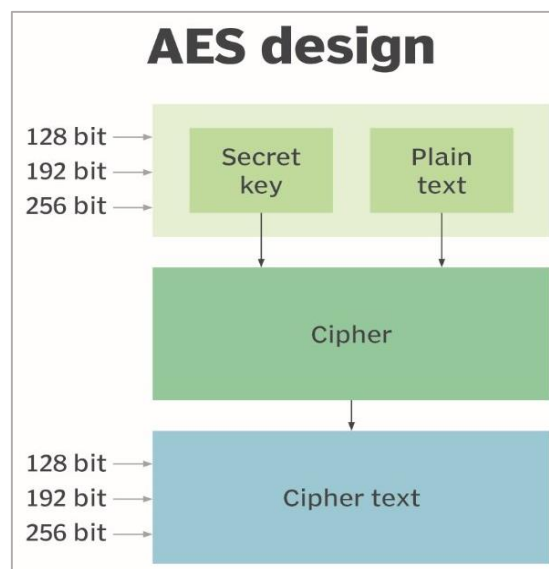


Fig. 2: AES Concept (Awati *et al.*, 2024)

Table 1: Table of strengths and weaknesses of UHC and AES

Aspect	UHC (Unimodular Hill Cipher)	AES (Advanced Encryption Standard)
Strengths	Simple to implement and understand	Highly secure and widely trusted for a variety of applications
	Flexible key size and easy integration with other techniques	Fast encryption and decryption, even for large data sizes
	Suitable for small-scale encryption needs	Resistant to various cryptanalysis techniques (e.g., brute force, differential cryptanalysis)
Weaknesses	Susceptible to attacks if the key is not properly managed	More complex than simpler ciphers, which can make implementation harder
	Performance can degrade with large matrices or image sizes	Requires a fixed key length and is computationally intensive for very small devices
	Less widely adopted, making it less tested in real-world scenarios	Requires efficient implementation to maintain speed
Security	Moderate security, dependent on the key size and management	Strong encryption, considered secure against most modern attacks
Efficiency	It can be less efficient for larger data due to matrix multiplication	High efficiency, especially for bulk encryption of large datasets
Flexibility	Allows for integration with other encryption techniques	Flexible key sizes (128, 192, 256 bits), allowing strong encryption options

Materials and Methods

In this session, we will explain some of the methods we use in this study. The proposed digital image encryption system uses a combination approach between Unimodular Hill Cipher and Advanced Encryption Standard (AES) (Muktyas *et al.*, 2021; Dooley, 2013). The workflow of encryption and decryption is the one in this study is as follows:

1. Preprocessing: Digital images are converted from a file format (e.g., PNG or JPEG) to a matrix representation, where each matrix element represents an image pixel. For color images, an RGB matrix is used (Zhang, 2022)
2. Unimodular hill cipher encryption: The image matrix is divided into small blocks according to the size of the selected key matrix. Each block is encrypted using a Unimodular Hill Cipher, where an unimodular key matrix is used to perform a linear transformation on each pixel block (Arifin *et al.*, 2022; Muktyas *et al.*, 2021; Lone and Qureshi, 2023)
3. AES encryption: The encryption results from the Unimodular Hill Cipher are passed to the AES algorithm. AES encrypts every block of data generated from Hill Cipher, ensuring that layered security is applied to the image (Hussein and Amintoosi, 2023; Singh and Jayanthi, 2019)
4. Decryption: The decryption process is carried out by reversing the encryption process, first using AES to decrypt the encrypted block and then using Unimodular Hill Cipher to return the original image matrix (Tan *et al.*, 2021; Arifin *et al.*, 2023a-b)
5. Post-processing: Once all the decryption blocks are complete, the image matrix is rearranged into a readable digital image (Pagano *et al.*, 2023)

The selection of keys and the approach of the unimodular concept to ensure the security of digital images are as follows:

- a. Selection of unimodular hill cipher locks: The unimodular key matrix is chosen in such a way that its determinants are worth ± 1 . This ensures that the matrix can be inverted without losing information, which is an important condition in the decryption process
- b. AES key selection: AES symmetric keys are selected according to the desired block length (128-bit, 192-bit, or 256-bit). AES uses complex substitution and randomization processes to keep data secure, ensuring that images remain protected from brute force or cryptographic attacks

The encryption algorithm and steps to implement the Unimodular Hill Cipher method and the integration process of the AES method as an additional algorithm to strengthen the security of the digital images used in this study are as follows (Jameel and Fadhel, 2022; Kanwal *et al.*, 2021):

1. Image to matrix conversion: Each pixel of a digital image is converted into a numerical value and organized in the form of a matrix (Acharya *et al.*, 2010)
2. Image blocks: The image matrix is divided into blocks according to the size of the predefined key matrix. For example, if the key matrix is 3x3 in size, the image will be divided into 3x3 blocks (Qobbi *et al.*, 2022)
3. Encryption with unimodular hill cipher: Each block is treated as a vector that will be multiplied by an unimodular key matrix. The result of this multiplication will be the ciphertext of the block (Arifin and Muktyas, 2021; Arifin and Muktyas, 2018)
4. Result: An encrypted image in the form of a matrix that has been randomized by the Unimodular Hill Cipher method
5. Cipher block conversion: The result of Unimodular Hill Cipher encryption is used as input for AES encryption (Paragas *et al.*, 2019)
6. AES encryption: The AES algorithm uses a pre-selected key to encrypt blocks of data originating from the Unimodular Hill Cipher (Chauhdary *et al.*, 2022)

7. AES will implement substitution, permutation, and randomization processes, making encrypted images more difficult to crack (Noor Muchsin *et al.*, 2019)
8. Decryption: On the receiver side, the encrypted block is first decrypted using AES, followed by the Unimodular Hill Cipher, to return the original image (Vinichenko *et al.*, 2021)

The implementation of Python code and the description of some Python libraries used in this study are as follows (Abdillah *et al.*, 2021):

- i) NumPy: Used to handle matrix and vector operations on digital images, especially in Unimodular Hill Cipher applications
- ii) Pillow (PIL): Used to read and manipulate digital images in common formats such as PNG, JPEG, etc.
- iii) PyCryptodome: Used for the implementation of AES in data encryption and decryption
- iv) Matplotlib: Used to visualize original and encrypted images and compare the results. The development of Python code for the process of encrypting and decrypting digital images has been incorporated into the researcher's Google Colab account, and readers can view and develop it by accessing the following link: <https://bit.ly/uhc-aes-image>. Further, the following Fig. (3) is a view of the proposed program code (Claudio *et al.*, 2022; Zhou *et al.*, 2021)

The following is a general summary of the menu provided in Fig. (3):

- a) Encryption: This section will handle the encryption process. Unimodular Hill Cipher is used as the first layer of encryption to map the original digital image to its initial encrypted form. After that, AES will be used as a second layer to increase security by utilizing encrypted symmetric keys
- b) Decryption: In this part, the decryption process is carried out. Digital images encrypted via AES will be decrypted first, followed by a Unimodular Hill Cipher decryption process to recover the original digital images
- c) Original text histogram and frequency analysis: Histogram analysis of the frequency of letters in the original digital image is performed to see the distribution of characters. This is useful in studying frequency patterns that can be helpful in cryptanalysis attacks on simpler encryption methods
- d) Encrypted text histogram and frequency analysis: After the encrypted digital image is encrypted, the letter frequency histogram of the encrypted digital image is generated. Typically, good encryption results in a more uniform distribution of characters, making frequency analysis more difficult

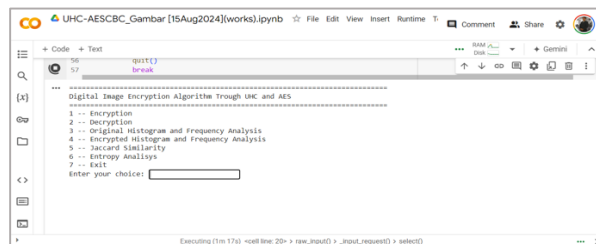


Fig. 3: Main program view

- e) Correlation analysis: This analysis measures the relationship between the original digital image and the encrypted digital image. A low or non-existent correlation is a strong sign of encryption because the relationship between the original digital image and the encrypted digital image should be unpredictable
- f) Speed and performance analysis: Here, you measure the speed and performance of encryption and decryption algorithms, comparing how long it takes to process a particular data, especially on large file sizes
- g) Entropy analysis: Entropy is a measure of uncertainty or randomness. The higher the entropy of an encrypted digital image, the more difficult it is to guess the patterns or characters that may be present, indicating the strength of the encryption
- h) Exit: This section will terminate the program (Kordov, 2021; Sutthisompohn and Kusol, 2021; Shamsa Kanwal *et al.*, 2022)

Results

In this session, the results and discussion of this study will be discussed. The original digital image source used to implement the program offered can be seen in the following Fig. (4), which has an image size of 1500'843 pixels and a file size of 164.3 KB.

Table (2) contains an analysis of the encryption process on the given digital image, which consists of changing password 1. The results of the study show that the larger the password 1, the greater the encryption time required. Furthermore, the results of the correlation analysis using Jaccard similarity show that there is no correlation between the original digital image and the encrypted digital image, which also means that a strong encryption process has occurred. On the other hand, in the entropy value column, the resulting values indicate that the encrypted digital image has good security from a cryptographic perspective because it is difficult for attackers to find patterns that can be used to break the encryption.



Fig. 4: Original digital image (Samdro, 2024)


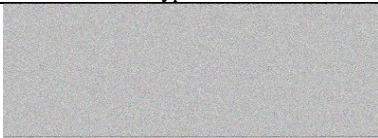
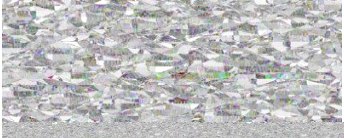
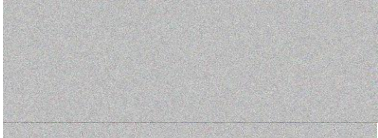



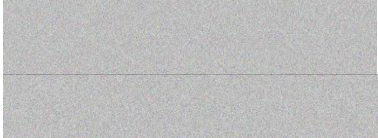
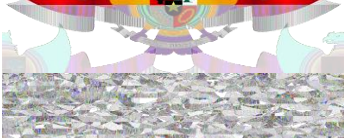

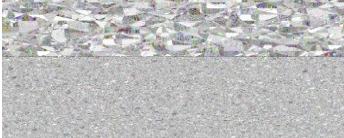
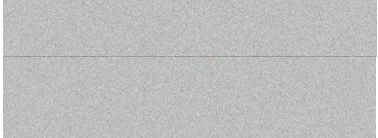




Table (3) is the result of the encryption of the digital image provided. With the password given, it will provide the result of encryption of digital images that are increasingly gray and difficult to distinguish from the original digital image. Further, the encrypted image shows that every element of the original image has been scrambled into a completely unrecognizable shape. The colors and patterns present in the original image have changed drastically

through an encryption process, making it a random look with no meaningful visual patterns. This change is due to an encryption algorithm that has changed the value of each pixel based on a unique encryption key. Thus, although the size and resolution of the image remain the same, its contents have been completely disguised so that no information can be retrieved directly from the encrypted image without the appropriate key to decrypt it.

Table 2: Analysis of time, correlation, and entropy

Password 1	Password 2	Encryption time (seconds)	Decryption time (seconds)	Encryption file size (Kbytes)	Jaccard similarity	The value of entropy
2	2020	0.897451162	1.312263727	4947.2640000	0.00	7.6314
20	2020	1.389388561	1.277773142	4947.2705000	0.00	7.6336
100	2020	1.924169302	1.784979343	4947.2773000	0.00	7.6314
900(max value)	2020	66.12623644	67.03863573	4947.2695300	0.00	7.6325
2	20202024	0.860365152	0.740767956	4947.2714800	0.00	7.6314
20	20202024	1.390430212	1.269494295	4947.2587890	0.00	7.6332
100	20202024	1.902062416	1.798160315	4947.2607421	0.00	7.6330
900(max value)	20202024	64.99629903	67.27529526	4947.2646400	0.00	7.6321

Table 3: Analysis of encrypted digital images

Password 1	Password 2	UHC encryption	UHC+AES encryption
2	2020		
20	2020		
100	2020		
900 (max value)	2020		
2	20202024		
20	20202024		
100	20202024		
900 (max value)	20202024		

Visual analysis showed that there was no indication of the original content of the image, which is evidence of the effectiveness of the encryption algorithm used. This encryption ensures that the image is protected from unauthorized data access attempts, providing high security in the storage and transmission of image data. The Table displays the relationship between Password 1 and Password 2, alongside the encryption results for two methods: UHC encryption and UHC + AES encryption. This Table highlights how varying password combinations impact the effectiveness of the encryption process on digital images, providing a clear comparison between the two encryption approaches.

Table (4) shows the results of histogram analysis of the colors of the given digital images and the images encrypted using the proposed UHC-AES method. Histogram analysis of the original image shows a highly focused distribution of pixels on a few specific color values with clearly visible frequencies. This indicates that the original image has areas with dominant colors or easily recognizable patterns. This uneven distribution of frequencies provides a visual clue about the content of the image. The image depicts the frequency distribution of pixel intensities for the Red, Green, and Blue (RGB) color channels in an image. Each histogram represents how often pixel intensity values (Ranging from 0-255) occur in the respective color channel. The red channel shows a concentration of pixels with low-intensity values, with a few spikes at higher values, indicating that the image contains predominantly dark red tones with sparse brighter red elements. Similarly, the green and blue channels display a similar pattern, where most pixels have

low-intensity values, suggesting the image is dominated by darker shades in these channels as well.

This distribution suggests that the image overall has a darker tone across all three channels, with limited bright colors. The sparse spikes at higher intensity values in each channel might represent isolated bright regions or specific color highlights in the image. These histograms are commonly used in image processing to analyze color distributions, adjust brightness and contrast, or identify patterns for further analysis, such as encryption, compression, or feature extraction tasks.

On the other hand, histogram analysis of encrypted images shows an almost uniform distribution of pixels across the color spectrum. There is no visible pattern or specific dominant area, which indicates that each pixel in the image has been effectively randomized by the encryption algorithm. Frequency analysis of encrypted images also showed more random results, where the distribution of intensity values was close to the same degree of freedom across the images. This is an indicator that the encryption algorithm is working well at disguising the content of the original image, eliminating visual patterns that can be used in image-based cryptanalysis attacks. Overall, the histogram and frequency comparison between the original and encrypted images shows the successful transformation of the structured image into a random image, increasing the security of the data it contains. This is stated in the following Table (5), especially for password one fixed and password two moving up and vice versa that presents the histogram analysis of encrypted images, which includes three key components: Password 1, 2, and the Encryption Histogram of UHC + AES.

Table 4: Histogram analysis of the original image

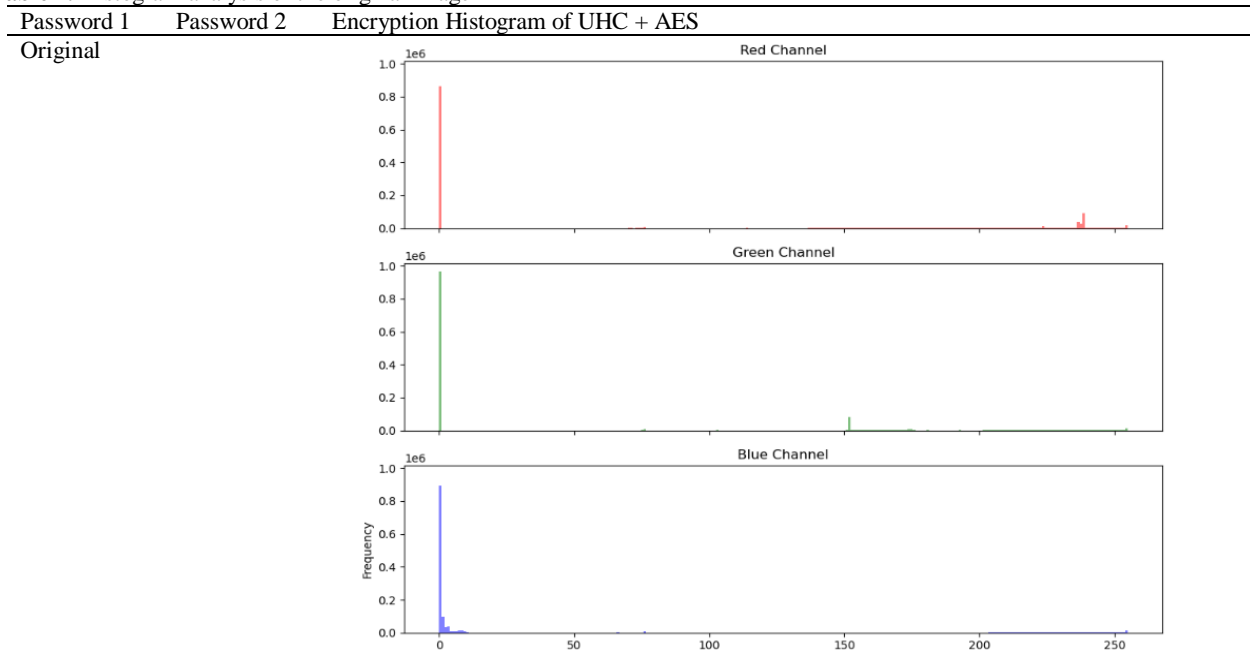
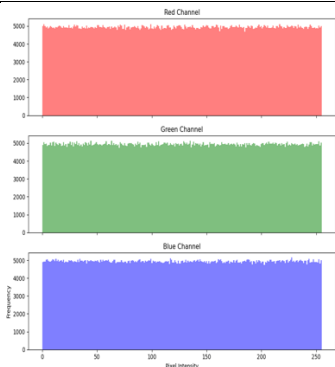
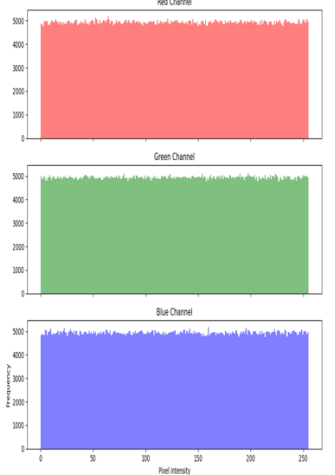


Table 5: Histogram analysis of encrypted images

Password 1	Password 2	Encryption histogram of UHC + AES
2	2020	
900	2020220 24	

These components illustrate the impact of different password inputs on the encryption process and highlight the distribution of pixel intensity values in the encrypted images generated using the combined Unimodular Hill Cipher (UHC) and Advanced Encryption Standard (AES) method. This analysis demonstrates the effectiveness of the hybrid encryption technique in producing randomized and uncorrelated pixel distributions, ensuring robust security for digital image encryption. Note that Table (5) will close this session.

Discussion

Some research talks about emerging security attacks and relates them to our work. For instance, Supersingular Isogeny Key Encapsulation (SIKE) employs fast isogeny accelerator architectures to achieve quantum resistance and IND-CCA security. However, its implementation must be constant to mitigate vulnerabilities such as timing and power analysis side-channel attacks. Similarly, Koblitz curve cryptography, designed for extremely constrained environments, leverages efficient hardware techniques like Gaussian Normal Basis (GNB) multipliers

to optimize performance. Despite their advantages, these techniques face risks from improper hardware design, such as vulnerabilities in rewiring or register sharing, which could lead to fault injection or differential attacks. Our work builds on these insights by integrating advanced cryptographic methods with fault detection mechanisms, enhancing security while maintaining performance in constrained applications (Koziel *et al.*, 2020; Azarderakhsh *et al.*, 2014).

Moreover, here is some research about fault detection and cryptography that relates to our work. Fault injection attacks pose a significant threat to cryptographic systems, particularly in disrupting encryption integrity. For example, parity-based fault detection schemes for S-boxes have been shown to effectively mitigate such vulnerabilities by maximizing error coverage with minimal overhead. Concurrent error detection methods, as demonstrated in secure implementations of SHA-3, enhance reliability by integrating precomputing mechanisms to withstand faults while maintaining performance efficiency. Similarly, side-channel attacks targeting non-linear S-boxes can be countered using Threshold Implementation (TI) techniques, which incorporate lightweight error detection through share-swapping. These advancements emphasize the critical role of robust fault and error detection strategies, aligning with our efforts to improve security and reliability in cryptographic systems (Kermani and Reyhani-Masoleh, 2006; Siavash *et al.*, 2014; Kermani *et al.*, 2018).

While our hybrid method demonstrates improved encryption efficiency, challenges persist. The computational overhead introduced by AES, particularly for high-resolution images, necessitates further optimization. Moreover, potential vulnerabilities in key exchange mechanisms require exploration to mitigate man-in-the-middle attacks in networked environments.

Conclusion

The conclusion of this study is as follows. The encryption process that is carried out shows the effectiveness of hiding the original information from images or text through the application of strong encryption algorithms. Using a combination of methods such as Unimodular Hill Cipher and AES, the original data was successfully transformed into an unrecognizable form, both visually and through statistical analysis. Histogram and frequency analysis showed that this encryption was able to eliminate patterns that are usually used for cryptanalysis, thus increasing the level of security. However, challenges remain, including optimizing encryption speeds for larger files and developing more efficient methods to keep data secure without sacrificing performance. Overall, the results of this study contribute positively to the improvement of

digital data security and open up opportunities for further research in the field of cryptography.

Although this study demonstrates the effectiveness of the combination of Unimodular Hill Cipher and AES methods in protecting digital data, some open issues still need to be investigated further. One of the main challenges is the efficiency of the algorithm when applied to large files, such as high-resolution images or complex audio-video data. Moreover, although encryption can disguise patterns from frequency analysis, the potential for artificial intelligence-based cryptanalysis attacks is still an unsolved threat. Another problem is the increased speed of decryption, which sometimes requires high computing power and can be a bottleneck in real-time applications. Future research needs to explore more efficient and secure hybrid algorithms, as well as consider methods to speed up the encryption and decryption process without sacrificing security levels.

Future work on this hybrid encryption system could explore the integration of machine-learning-driven anomaly detection mechanisms to identify and mitigate cryptographic attacks in real-time. Additionally, optimized versions of the proposed method could be developed to enhance encryption and decryption efficiency for real-time multimedia streaming applications. Furthermore, the system's performance should be analyzed within quantum-safe cryptographic frameworks to ensure resilience against emerging threats posed by quantum computing advancements.

Acknowledgment

The authors would like to thank the reviewers for their insightful comments, suggestions, and ideas, which have greatly contributed to improving this manuscript and making it suitable for publication. Their dedication to advancing research in the fields of data science and cryptography is deeply appreciated.

Funding Information

This study was supported and funded by the Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM), Institut Teknologi Sains Bandung (ITSB). Additionally, the fifth author would like to extend special thanks to the Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) at Universitas Ahmad Dahlan (UAD) for their internal research funding, provided under contract number PT-117/SP3/LPPM-UAD/XI/2024.

Author's Contributions

Samsul Arifin: Contributed the core idea of a new encryption framework. He introduced a hybrid encryption scheme that combines the Unimodular Hill Cipher and

Advanced Encryption Standard (AES) to enhance image security while maintaining computational efficiency.

Dwi Wijonarko: Improved the system's security by utilizing unimodular matrices in the Hill Cipher to overcome the invertibility limitations of the standard cipher and to increase resistance to known plaintext attacks.

Monica Mayeni Manurung: Developed an integration method with AES to improve robustness. She designed a system where the Unimodular Hill Cipher preprocesses image data before AES encryption, providing a dual-layer encryption mechanism for enhanced security.

Roni: Conducted a comprehensive security analysis, including both theoretical and empirical evaluations such as key sensitivity tests, encryption quality assessments, and statistical resistance tests, to validate the strength of the proposed scheme.

Puguh Wahyu Prasetyo: Focused on optimizing efficiency. He implemented the proposed method and improved its computational performance, demonstrating its practicality for real-time image encryption applications.

Fabian Surya Pramudya: Highlighted the real-world applications of the proposed encryption framework. He emphasized its potential use in secure image transmission, medical imaging, and cloud-based image storage, addressing practical challenges in these areas.

Ethics

This manuscript reports original research and includes content that has not been previously published. The corresponding author confirms that there are no conflicts of interest related to this study and that it raises no ethical issues.

References

- Abdillah, A. A., Azwardi, A., Permana, S., Susanto, I., Zainuri, F., & Arifin, S. (2021). Performance evaluation of linear discriminant analysis and support vector machines to classify cesarean section. *Eastern-European Journal of Enterprise Technologies*, 5(2 (113)), 37-43. <https://doi.org/10.15587/1729-4061.2021.242798>
- Acharya, B., Sharma, M. D., Tiwari, S., & Minz, V. K. (2010). Privacy Protection of Biometric Traits Using Modified Hill Cipher with Involutory Key and Robust Cryptosystem. *Procedia Computer Science*, 2, 242-247. <https://doi.org/10.1016/j.procs.2010.11.031>
- Arifin, A. S., Alabdullah, B., Alqahtani, Hamed, Aljameel, S. S., Alotaibi, S. S., & Mohamed, A. (2023a). Algorithm for Digital Image Encryption Using Multiple Hill Ciphers, a Unimodular Matrix and a Logistic Map. *Heliyon*, 11(6S), 311-324. <https://doi.org/https://www.ijisae.org/index.php/IJISAE/article/view/2858>

- Arifin, S., & Muktyas, I. B. (2018). Membangkitkan Suatu Matriks Unimodular Dengan Python. *Jurnal Derivat: Jurnal Matematika Dan Pendidikan Matematika*, 5(2), 1-9.
<https://doi.org/10.31316/j.derivat.v5i2.361>
- Arifin, S., Muktyas, I. B., Prasetyo, P. W., & Abdillah, A. A. (2021). Unimodular matrix and bernoulli map on text encryption algorithm using python. *Al-Jabar: Jurnal Pendidikan Matematika*, 12(2), 447-455.
<https://doi.org/10.24042/ajpm.v12i2.10469>
- Arifin, S., & Muktyas, I. B. (2021). Generate a System of Linear Equation Through Unimodular Matrix Using Python and Latex. *AIP Conference Proceedings*. The 2nd Science and Mathematics International Conference (SMIC 2020): Transforming Research and Education of Science and Mathematics in the Digital Age, Jakarta, Indonesia.
<https://doi.org/10.1063/5.0041651>
- Awati, R., Bernstein, C., & Cobb, M. (2024). Advanced Encryption Standard (AES). *TechTarget*.
<https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>
- Arifin, S., Wijonarko, D., Suwarno, & Sijabat, E. K. (2024). Application of Unimodular Hill Cipher and RSA Methods to Text Encryption Algorithms Using Python. *Journal of Computer Science*, 20(5), 548–563.
<https://doi.org/10.3844/jcssp.2024.548.563>
- Arifin, S., Kurniadi, F. I., Yudistira, I. G. A., Nariswari, R., Murnaka, N. P., & Muktyas, I. B. (2022). Image Encryption Algorithm Through Hill Cipher, Shift 128 Cipher and Logistic Map Using Python. *2022 3rd International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, 221-226.
<https://doi.org/10.1109/aidas56890.2022.9918696>
- Azanuddin, A., Kartadie, R., Erwis, F., Boy, A. F., & Nasyuha, A. H. (2024). A Combination of Hill Cipher and RC4 Methods for Text Security. *Telkomnika (Telecommunication Computing Electronics and Control)*, 22(2), 351–361.
<https://doi.org/10.12928/telkomnika.v22i2.25628>
- Azarderakhsh, R., Jarvinen, K. U., & Mozaffari-Kermani, M. (2014). Efficient Algorithm and Architecture for Elliptic Curve Cryptography for Extremely Constrained Secure Applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(4), 1144-1155.
<https://doi.org/10.1109/tcsi.2013.2283691>
- Arifin, S., Tan, K., Ariani, A. T., Rosdiana, S., & Abdullah, M. N. (2023b). The Audio Encryption Approach uses a Unimodular Matrix and a Logistic Function. *International Journal of Emerging Technology and Advanced Engineering*, 13(4), 71-81.
https://doi.org/10.46338/ijetae0423_08
- Basavaiah, J., Anthony, A. A., & Patil, C. M. (2021). Visual Cryptography Using Hill Cipher and Advanced Hill Cipher Techniques. *Lecture Notes in Electrical Engineering*, 752, 429-443.
https://doi.org/10.1007/978-981-16-0443-0_34
- Chauhdary, S. H., Alkathairi, M. S., Alqarni, M. A., & Saleem, S. (2022). (Retracted) Improved Encrypted AI Robot for Package Recognition in LOT Logistics Environment. *Journal of Electronic Imaging*, 31(06).
<https://doi.org/10.1117/1.jei.31.6.061813>
- Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical Study of Hybrid Techniques for Image Encryption and Decryption. *Sensors*, 20(18), 5162-5448.
<https://doi.org/10.3390/s20185162>
- Dooley, J. F. (2013). The Machines Take Over: Computer Cryptography. *History of Cryptography and Cryptanalysis: Codes, Ciphers and Their Algorithms*, 9783319016, 167-184.
https://doi.org/10.1007/978-3-319-01628-3_8
- Hussein, M. K., & Amintoosi, H. (2023). Protection of Images by Combination of Vernam Stream Cipher, AES and LSB Steganography in a Video Clip. *Bulletin of Electrical Engineering and Informatics*, 12(3), 1578-1585.
<https://doi.org/10.11591/eei.v12i3.4039>
- Jameel, E. A., & Fadhel, S. A. (2022). Digital Image Encryption Techniques: Article Review. *Technium: Romanian Journal of Applied Sciences and Technology*, 4(2), 24-35.
<https://doi.org/10.47577/technium.v4i2.6026>
- Kanwal, S., Inam, S., Cheikhrouhou, O., Mahnoor, K., Zaguia, A., & Hamam, H. (2021). Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes. *Complexity*, 2021(1).
<https://doi.org/10.1155/2021/5499538>
- Kermani, M. M., Jalali, A., & Azarderakhsh, R. (2018). Lightweight Error Detection Architectures through Swapping the Shares for a Subset of S-boxes. *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, 578–581.
<https://doi.org/10.1109/mwscas.2018.8624009>
- Kermani, M., & Reyhani-Masoleh, A. (2006). Parity-Based Fault Detection Architecture of S-box for Advanced Encryption Standard. *2006 21st IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*. 2006 21st IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Arlington, VA, USA.
<https://doi.org/10.1109/dft.2006.50>
- Kordov, K. (2021). Text Encryption Algorithm for Secure Communication. *International Journal of Applied Mathematics*, 34(4).
<https://doi.org/10.12732/ijam.v34i4.9>

- Koziel, B., Ackie, A.-B., Khatib, R. E., Azarderakhsh, R., & Kermani, M. M. (2020). SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 67(12), 4842-4854. <https://doi.org/10.1109/tcsi.2020.2992747>
- Koziel, B., Azarderakhsh, R., & Kermani, M. M. (2018). A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. *IEEE Transactions on Computers*, 67(11), 1594-1609. <https://doi.org/10.1109/tc.2018.2815605>
- Koziel, B., Azarderakhsh, R., & Mozaffari-Kermani, M. (2016). Fast Hardware Architectures for Supersingular Isogeny Diffie-Hellman Key Exchange on FPGA. *Progress in Cryptology – INDOCRYPT 2016*, 10095, 191-206. https://doi.org/10.1007/978-3-319-49890-4_11
- Lone, M. A., & Qureshi, S. (2023). Encryption Scheme for RGB Images Using Chaos and Affine Hill Cipher Technique. *Nonlinear Dynamics*, 111(6), 5919-5939. <https://doi.org/10.1007/s11071-022-07995-2>
- Lone, P. N., & Singh, D. (2020). Application of Algebra and Chaos Theory in Security of Color Images. *Optik*, 218, 165155. <https://doi.org/10.1016/j.jileo.2020.165155>
- Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., Mir, U. H., & Kumar, N. (2022). Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. *Mathematics*, 10(20), 3878-3919. <https://doi.org/10.3390/math10203878>
- Muktyas, I. B., Sulistiawati, & Arifin, S. (2021). Digital Image Encryption Algorithm Through Unimodular Matrix and Logistic Map using Python. *AIP Conference Proceedings*. The 2nd Science and Mathematics International Conference (Smic 2020): Transforming Research and Education of Science and Mathematics in The Digital Age, Jakarta, Indonesia. <https://doi.org/10.1063/5.0041653>
- National Institute of Standards and Technology (US). (2023). *Advanced Encryption Standard (AES)*. <https://doi.org/10.6028/nist.fips.197-upd1>
- Nishimwe, A., Ruranga, C., Musanabaganwa, C., Mugeni, R., Semakula, M., Nzabanita, J., Kabano, I., Uwimana, A., Utumatwishima, J. N., Kabakambira, J. D., Uwineza, A., Halvorsen, L., Descamps, F., Houghtaling, J., Burke, B., Bahati, O., Bizimana, C., Jansen, S., Twizere, C., Twagirumukiza, M. (2022). Leveraging Artificial Intelligence and Data Science Techniques in Harmonizing, Sharing, Accessing and Analyzing SARS-COV-2/COVID-19 Data in Rwanda (LAISDAR Project): Study Design and Rationale. *BMC Medical Informatics and Decision Making*, 22(1). <https://doi.org/10.1186/s12911-022-01965-9>
- Noor Muchsin, H. N., Sari, D. E., Ignatius Moses Setiadi, D. R., & Rachmawanto, E. H. (2019). Text Encryption using Extended Bit Circular Shift Cipher. *2019 Fourth International Conference on Informatics and Computing (ICIC)*. 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia. <https://doi.org/10.1109/icic47613.2019.8985708>
- Pagano, T. P., Loureiro, R. B., Lisboa, F. V. N., Peixoto, R. M., Guimarães, G. A. S., Cruz, G. O. R., Araujo, M. M., Santos, L. L., Cruz, M. A. S., Oliveira, E. L. S., Winkler, I., & Nascimento, E. G. S. (2023). Bias and Unfairness in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics and Identification and Mitigation Methods. *Big Data and Cognitive Computing*, 7(1), 15. <https://doi.org/10.3390/bdcc7010015>
- Paragas, J. R., Sison, A. M., & Medina, R. P. (2019). A New Variant of Hill Cipher Algorithm Using Modified S-Box. *Int. J. Sci. Technol. Res*, 8(10), 615-619.
- Qobbi, Y., Jarjar, A., Essaid, M., & Benazzi, A. (2022). *New Image Encryption Scheme Based on Dynamic Substitution and Hill Cipher*. 797-808. https://doi.org/10.1007/978-981-33-6893-4_72
- Siavash, B.-S., Mehran Mozaffari, K., & Reyhani-Masoleh, A. (2014). Efficient and Concurrent Reliable Realization of the Secure Cryptographic SHA-3 Algorithm. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(7), 1105-1109. <https://doi.org/10.1109/tcad.2014.2307002>
- Sreejith, R., & Senthil, S. (2021). Framework for Concealing Medical Data in Images Using Modified Hill Cipher, Multi-Bit EF and ECDSA. *International Journal of Information and Communication Technology*, 19(2), 168-183. <https://doi.org/10.1504/ijict.2021.117044>
- Samodro, D. B. (2024). File:GARUDA PANCASILA.jpg. *Commons*. Accessed: Jul. https://commons.wikimedia.org/wiki/File:GARUDA_PANCASILA.jpg
- Shamsa Kanwal, Inam, S., Hajje, F., Cheikhrouhou, O., Nawaz, Z., Waqar, A., & Khan, M. (2022). A New Image Encryption Technique Based on Sine Map, Chaotic Tent Map and Circulant Matrices. *Security and Communication Networks*, 2022, 1-17. <https://doi.org/10.1155/2022/4152683>
- Singh, K. J., & Jayanthi, R. (2019). A Public Key-Based Encryption and Signature Verification Model for Secured Image Transmission in Network. *International Journal of Internet Technology and Secured Transactions*, 9(3), 299. <https://doi.org/10.1504/ijitst.2019.10023424>

- Sharma, A., Singh, A., & Kumar, A. (2022). Encryption and Decryption of Marker Based 3-Dimensional Augmented Reality Image Using Modified Hill Cipher Technique for Secure Transfer. *2022 IEEE 2nd International Conference on Computer Communication and Artificial Intelligence (CCAI)*. Beijing, China.
<https://doi.org/10.1109/ccai55564.2022.9807727>
- Subramanian, S., Mozaffari-Kermani, M., Azarderakhsh, R., & Nojournian, M. (2017). Reliable Hardware Architectures for Cryptographic Block Ciphers LED and HIGHT. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36(10), 1750-1758. <https://doi.org/10.1109/tcad.2017.2661811>
- Suryadi, M., Satria, Y., & Hadidulqawi, A. (2021). Implementation of the Gauss-Circle Map for encrypting and embedding simultaneously on digital image and digital text. *Journal of Physics: Conference Series*, 1821(1), 012037.
<https://doi.org/10.1088/1742-6596/1821/1/012037>
- Sutthisompohn, S., & Kusol, K. (2021). Association Between Caregivers' Family Management and Quality of Life in Children with Chronic Disease in Southern Thailand. *Patient Preference and Adherence, Volume 15*, 2165-2174.
<https://doi.org/10.2147/ppa.s327553>
- Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series*, 1997(1), 012021.
<https://doi.org/10.1088/1742-6596/1997/1/012021>
- Claudio, B. M., Tapia, L. N., & Díaz, W. A. (2022). Graphical Interface to Improve Python Language Teaching and Image Processing. *International Journal of Emerging Technology and Advanced Engineering*, 12(3), 92-98.
https://doi.org/10.46338/ijetae0322_10
- Vinichenko, M. V., Vinogradova, M. V., NikiporetsTakigawa, G. Yu., & Rybakova, M. V. (2021). The Impact of the Pandemic on the Quality of Education and the Image of a University. *XLinguae*, 14(1), 17-37.
<https://doi.org/10.18355/xl.2021.14.01.02>
- Zhang, X. (2022). Application of Artificial Intelligence Recognition Technology in Digital Image Processing. *Computer Science*, 2022.
<https://doi.org/10.1155/2022/7442639>
- Zhou, Y., Wang, J., Zuo, R., Xiao, F., Shen, W., & Wang, S. (2021). Machine Learning, Deep Learning and Implementation Language in Geological Field. *Journal of Autonomous Intelligence*, 4(1), 6.
<https://doi.org/10.32629/jai.v4i1.479>