Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 9, No. 3, August, Pp. 267-276

A super-encryption approach for enhancing digital security using column transposition - hill cipher for 3D image protection

Lekso Budi Handoko[*1], **Chaerul Umam**[1]
University of Dian Nuswantoro, Indonesia[1]

Article Info

Keywords:
Columnar Transposition, Hill Cipher, Image Encryption, Quality Measurement, Super Encryption

Article history:
Received: February 24, 2024
Accepted: May 30, 2024
Published: August 31, 2024

Cite:
L. B. Handoko and C. Umam, “A Super Encryption Approach for Enhancing Digital Security using Column Transposition - Hill Cipher for 3D Image Protection”, KINETIK, vol. 9, no. 3, Aug. 2024. https://doi.org/10.22219/kinetik.v9i3.1984

*Corresponding author.
Lekso Budi Handoko
E-mail address:
handoko@dsn.dinus.ac.id

Abstract

Image encryption is an indispensable technique in the realm of information security, serving as a pivotal mechanism to safeguard visual data against unauthorized access and potential breaches. This study scrutinizes the effectiveness of merging columnar transposition with the Hill Cipher methodologies, unveiling specific metrics from a curated set of sample images. Notably, employing column transposition with the key "JAYA" and the Hill Cipher with the key "UDINUSSMG," the encrypted images underwent rigorous evaluation. 'Lena.png' demonstrated an MSE of 513.32 with a PSNR of 7.89 dB, while 'Peppers.png' and 'Baboon.png' recorded MSE values of 466.67 and 423.92, respectively, with corresponding PSNR figures of 7.12 dB and 7.31 dB. Across all samples, a consistent BER of 50.00% indicated uniform error propagation, while entropy values settled uniformly at 7.9999, highlighting consistent data complexity. While the findings underscore a consistent error rate and complexity, there's a compelling need for further refinement to enhance image quality and security. Moreover, the study proposes future research avenues exploring a three-layer super encryption paradigm, amalgamating columnar transposition, Hill Cipher, and other robust algorithms. This approach aims to fortify encryption methodologies against evolving threats and challenges in data protection, offering heightened resilience and efficacy in safeguarding sensitive information.

1. Introduction

Image encryption is an indispensable technique in the realm of information security, serving as a pivotal mechanism to safeguard visual data against unauthorized access and potential breaches [1], [2], [3]. Commencing with the fundamental premise that the integrity and confidentiality of digital imagery must be upheld, image encryption methodologies employ intricate algorithms to transform pixel values, thereby obscuring the underlying content [4], [5]. This transformation process ensures that the visual representation remains indecipherable to unintended recipients, thereby preserving the privacy and authenticity of the image [4], [6]. When attackers resort to brute force methods, the benefits of using a two-step encryption system like super encryption become incredibly valuable. By encrypting data in consecutive stages with techniques such as column transposition and the Hill cipher, this approach significantly complicates the task for intruders trying to decrypt the information [7], [8]. Not only do they have to crack the code for one encryption method, but they also have to figure out the correct sequence of these methods. This adds a layer of complexity that makes brute-force attacks much more challenging and time-consuming. Essentially, super-encryption acts as an extra shield, making it harder for attackers to breach and access sensitive data effortlessly [9].

Based on the problem analysis, research objective in this study is to adopt a cutting-edge super-encryption approach that combines the methodologies of column transposition and the Hill cipher, marking a novel advancement in the realm of digital image security [10], [11]. The procedure commenced with the initial data processing utilizing the column transposition technique, yielding encrypted image outcomes based on its specific principles. Following this primary encryption phase, we further enhanced the security measures by subjecting the processed data to secondary encryption using the Hill cipher [2], [3], [12], [13]. The synergistic integration of these two encryption techniques establishes an additional layer of formidable security, rendering the decryption process more intricate and bolstering the safeguarding of encoded information. The distinctiveness of this approach lies in its intelligent amalgamation of column transposition and the Hill cipher, culminating in a fortified and secure solution for preserving the integrity and confidentiality of digital images [14], [15]. Consequently, this methodological innovation signifies a pivotal stride forward in the enhancement of digital image security protocols, elevating the efficacy and resilience of our digital security infrastructure. In adopting a super-encryption approach that combines column transposition and the Hill Cipher methodologies, several strategic considerations underline their selection as primary encryption techniques. Firstly, column transposition offers simplicity and efficiency in rearranging pixel values within an image, providing a foundational layer of encryption. This technique, with its key "JAYA," introduces randomness and complexity, deterring brute-force attacks while maintaining manageability for users. Secondly, the Hill Cipher, utilizing the key "UDINUSSMG," complements column transposition by adding a sophisticated layer of encryption through matrix operations. Its mathematical complexity enhances security by scrambling image data intricately, further fortifying the encryption process. These techniques establish a formidable security posture, rendering decryption more intricate and bolstering the safeguarding of encoded information. The amalgamation of column transposition and the Hill Cipher signifies a significant advancement in digital image security, offering a balance between simplicity and sophistication. This methodological innovation not only elevates the efficacy and resilience of digital security infrastructure but also underscores their relevance and effectiveness compared to alternative encryption approaches, thus marking a pivotal stride forward in enhancing digital image security protocols.

Numerous researchers are increasingly adopting the innovative approach of super-encryption, marking a significant advancement in contemporary cryptographic methodologies. Research by Putrie [2] highlights the ongoing advancements in cryptography, especially when it comes to securing digital images. The Hill cipher stands out as a widely recognized and utilized cryptographic algorithm, commonly employed in various studies to decrypt data effectively. Recognizing the need to continually enhance security measures in line with technological progress, this study ventured into merging the capabilities of the Hill cipher with the column transposition method. By initially applying column transposition, the image undergoes a randomization process, followed by the Hill algorithm, which substitutes specific values within the image. This innovative blend of randomization and value substitution techniques results in a super-encryption approach that demonstrates increased resilience against diverse cyber-attacks. The study's empirical evaluations, incorporating metrics like PSNR, MSE, SSIM, entropy, and encrypted image histograms, provide compelling evidence of the method's superiority over singular or combined application strategies of the transposition method and Hill cipher. Research by Fadlan [16] delved into a fascinating approach by implementing a three-layer algorithm for super-encryption. This study recognized the challenges of maintaining robust data security in the context of Era Society 5.0, especially when relying solely on classical cryptography methods like substitution and transposition techniques. By ingeniously combining the strengths of the Autokey Cipher, Columnar Transposition, and Hill Cipher, Fadlan introduced what is termed the three-layer encryption protocol. Through rigorous evaluation using the Avalanche Effect approach, the outcomes were illuminating. The research concluded that this multifaceted encryption strategy provided notably enhanced security measures compared to conventional single-layer encryption methods, marking a significant advancement in safeguarding sensitive data in contemporary digital landscapes. Research by Budiman [17], explored the fascinating world of cryptography, distinguishing between its traditional and contemporary approaches. While older methods like the Zig-zag Cipher have served their purpose, they've also shown vulnerabilities. To address this, Budiman took a fresh approach by blending the Zig-zag Cipher with the more modern RC4+ Cipher, creating what's known as a super-encryption method. Essentially, this combination beefs up the security, making it much more challenging for anyone trying to crack the code. What stood out from the study was that when these two methods were combined, the complexity level increased significantly, making it even more robust against potential decryption efforts. In essence, Budiman's research offers a valuable step forward in strengthening our digital security measures.

In this research endeavor, while drawing parallels with the methodologies of the aforementioned three studies, the primary focus pivots toward the critical assessment of encryption quality through metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Bit Error Rate (BER), and entropy. The overarching objective of this investigation is to meticulously evaluate the efficacy and quality of the encryption mechanisms deployed, utilizing standardized quality assessment tools. By harnessing these specific metrics, the research aims to furnish a nuanced understanding of both the strengths and potential limitations inherent in the chosen encryption approaches. Through a comprehensive analysis grounded in MSE, PSNR, BER, and entropy evaluations, this study endeavors not only to delineate the performance metrics but also to proffer insights for refining and optimizing digital security protocols in an ever-evolving landscape.

2. Research Method

2.1 Columnar Transposition Algorithm

Columnar Transposition Algorithm is like a secret rearranging tool for images, making them harder for unauthorized eyes to understand. Imagine taking an image and jumbling up its pixels or sections based on a special sequence or key you've chosen [2]. That is essentially what this algorithm does. By using this method, the original layout and content of the image get scrambled, making it challenging for anyone without the specific key to decipher or make sense of it. In simpler terms, it is like turning your image into a puzzle that only someone with the right "instructions" or key can put back together. This technique is a go-to for boosting image security, ensuring that only those with the correct key can view the image in its original form [2], [18]. The flow of columnar Transposition can be seen below:

1. First, pick a key, like "JAYA" to guide the rearrangement.
2. Next, turn this key into a sequence of numbers. So, using "JAYA" might give the sequence [2, 1, 3, 4].
3. Now, take a message or data and break it into columns, following the length of your keyword. If the key has four letters, the data has four columns.

4. Then, shuffle these columns around based on the number sequence from the key. Think of it like moving columns of data around based on this secret number pattern.
5. Finally, put these columns back together from left to right, and get the encrypted image.

While this provides a structured overview, the actual process doesn't have a single mathematical equation but rather a series of steps that leverage the chosen keyword to determine the rearrangement pattern. The pixel randomization using columnar transposition can be seen in Figure 1.

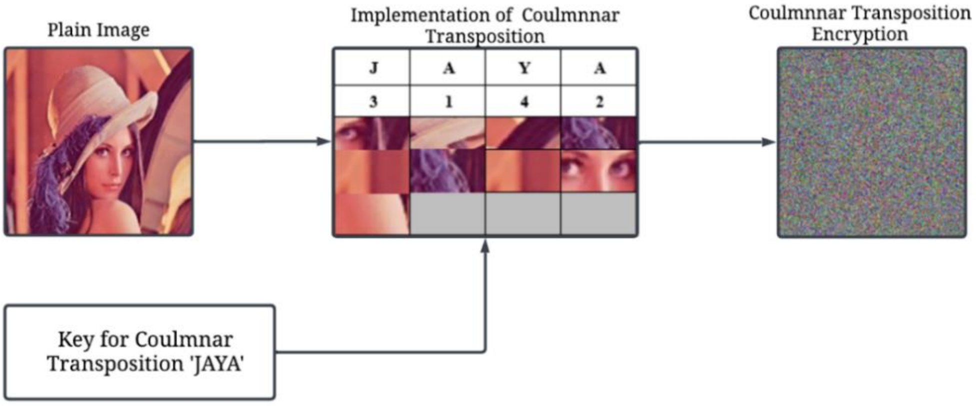

Plain Image
Implementation of Coulmnnar Transposition
J
A
Y
A
3
1
4
2
Coulmnnar Transposition Encryption
Key for Coulmnar Transposition 'JAYA'

Figure 1. Columnar Transposition Randomize by Pixel

The key "JAYA" is chosen for its ease of use and memorization, providing practicality and reducing the probability of errors. Its length determines the number of columns, offering flexibility for various data lengths. The resulting sequence [2, 1, 3, 4] adds randomness to the encryption, enhancing security by making decryption more challenging. Each column undergoes a unique permutation, increasing complexity. In summary, "JAYA" and [2, 1, 3, 4] strike a balance between simplicity, usability, and security, ideal for columnar transposition in image encryption.

2.2 Hill Cipher Algorithm

Hill Cipher algorithm is a sophisticated mechanism within image encryption, employing matrices and mathematical operations to bolster security measures[12]. For this specific encryption, the chosen key is "UDINUSSMG." Initially, this key is transformed into a matrix format to facilitate the encryption process. Subsequently, the image data is converted into corresponding matrices based on predefined parameters. Once these matrices are established, they undergo multiplication with the matrix derived from the "UDINUSSMG" key. Through this matrix multiplication process, the algorithm adeptly scrambles the image data uniquely and intricately, making decryption without the correct key notably challenging. In essence, by harnessing mathematical principles and matrix transformations, especially with the specific key "UDINUSSMG," the Hill Cipher algorithm furnishes a robust layer of security. This ensures the preservation of the integrity and confidentiality of the digital imagery, mitigating risks from unauthorized access or decryption attempts effectively. Hill Cipher operates on matrix multiplication, making it a unique encryption method. The Hill Cipher Equation 1 and Equation 3 can be seen below.

Key Matrix (K): This is the matrix derived from the keyword, such as "UDINUSSMG." It is a square matrix, typically of size n×n where n is determined by the length of the keyword. For "UDINUSSMG," the key matrix K would be derived as in (1). Plain Text Vector (P): The image or data is converted into a column vector where each element represents a value or pixel intensity.

$$K = \begin{pmatrix} 21 & 4 & 8 \\ 13 & 20 & 6 \\ 12 & 12 & 7 \end{pmatrix} \tag{1}$$

$$P = \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \tag{2}$$

The "UDINUSSMG" key was chosen strategically for the Hill Cipher algorithm due to its nine-character length, resulting in a 3x3 key matrix, balancing security and efficiency. The key's diverse mix of uppercase letters ensures randomness and complexity, reducing the possibility of cryptographic attacks. Its deliberate arrangement minimizes patterns, enhancing security against known-plaintext attacks. Overall, "UDINUSSMG" aligns with cryptographic best practices, maximizing the security of the encryption process for digital imagery.

It is essential to note that while the descprition above provides a general representation, an actual implementation might involve additional steps, such as ensuring the key matrix is invertible, handling block sizes, and managing edge cases. The hill cipher processing can be seen in Figure 2.

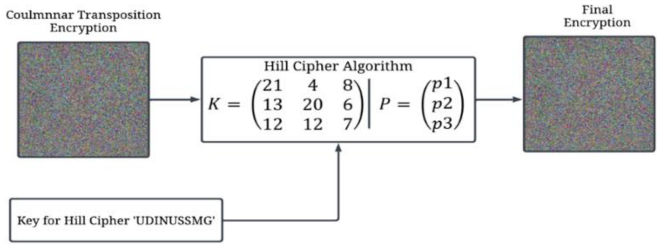

Coulmnnar Transposition Encryption
Hill Cipher Algorithm
$K = \begin{pmatrix} 21 & 4 & 8 \\ 13 & 20 & 6 \\ 12 & 12 & 7 \end{pmatrix} \Big| \; P = \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix}$
Final Encryption
Key for Hill Cipher 'UDINUSSMG'

Figure 2. Hill Cipher Processing

2.3 Proposed Method

In our proposed method, the first step is setting up our keys: 'JAYA' for the column transposition and 'UDINUSSMG' for the Hill cipher. Once those keys are in place, we kick off the encryption process. First up, we use the 'JAYA' key to encrypt the image through column transposition. After that initial encryption, we take it a step further by running that already encrypted image through another round of encryption, this time using the Hill cipher with the 'UDINUSSMG' key. Essentially, it is like adding an extra layer of protection to ensure that the image remains secure and unreadable to anyone trying to snoop around. The proposed scheme can be seen in Figure 3.

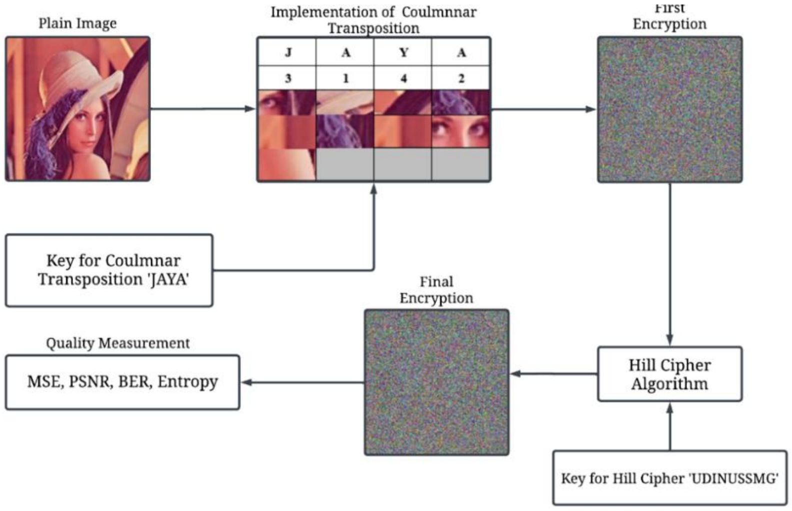


Figure 3. Proposed Scheme

2.4 Quality Measurement

When it comes to figuring out how good an image looks after the compression or processing, there are some go-to measures that experts use. First up is the Mean Squared Error (MSE), which gives an average of how much the compressed image differs from the original one [19]. A lower MSE means the two images are pretty similar. Then, there is the Peak Signal-to-Noise Ratio (PSNR), which is like the gold standard for many. It gives a kind of grade, with a higher PSNR indicating that the compressed image retains a lot of its original quality. The Bit Error Rate (BER) is another essential measure; it checks how many mistakes pop up in the compressed data compared to what was initially there [16], [20], [21], [22]. Lastly, there is Entropy, which looks at how complex or random the image data is [19], [23].

Think of it like this: if the image has a high entropy, it means a lot is going on, and it' is packed with information [24], [25]. So, by considering MSE, PSNR, BER, and Entropy together, experts get a well-rounded view of how well an image holds up through different processes. The quality measurement Equations 3 to 6 can be seen below.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (I(i,j) - K(i,j))^{2} \quad (3)$$

$$PSNR = 10 \log 10 \left(\frac{\max \_pixel\_value^{2}}{MSE} \right) \quad (4)$$

$$Entropy = -\sum_{i=1}^{n} P(x_i) \cdot Log_2(P(x_i)) \tag{5}$$

$$BER = \frac{Total\ number\ of\ incorrectly\ embedded\ bits}{Total\ Number\ of\ message\ Bits} \times 100 \tag{6}$$

3. Results and Discussion

During the testing phase, the team used MATLAB 2020a as the main software tool. To make sure everything ran smoothly, they had some solid hardware on their side: a 12th-generation i3 processor, an RTX 2060 Super graphics card, 16GB of RAM, and a speedy 512GB SSD. For the actual tests, they picked three classic images: Lena, Peppers, Baboon, Airplane, and Cameraman. These images were saved in .png format and kept at a consistent size of 512x512x3 pixels. With this setup, they were all set to dive deep and analyze how well the encryption worked, using key metrics like MSE, PSNR, BER, and Entropy to gauge performance and quality. The sample plain image can be seen in Figure 4.

(a) Lena (b) Baboon (c) Peppers (d) Airplane (e) Cameraman

Figure 4. Sample of Cover Image

Details from Figure 5 are laid out and explained further in Table 1. Think of Table 1 as a handy summary that breaks down what is shown in the figure. By looking at both the figure and the table, you get a full understanding of what the results are showing, giving you a clearer picture of the research findings.

Table 1. Results of Encrypted Image

Sample Image	MSE	PSNR	BER	Entropy
Lena.png	513.32	7.89 dB	50.00%	7.9999
Peppers.png	466.67	7.12 dB	50.01%	7.9999
Baboon.png	423.92	7.31 dB	50.00%	7.9999
Airplane.png	501.20	7.67 dB	50.00%	7.9999
Cameraman.png	333.42	8.22 dB	50.00%	7.9999

The outcomes from the testing phase using the related method stand out as the most optimal among the three research studies, as depicted and consolidated in Table 2. This table provides a comparative representation, emphasizing the superior results achieved through this specific approach compared to its counterparts.

Table 2. Results of Encrypted Image

Research	Sample Image	MSE	PSNR	BER	Entropy
Proposed Method	Lena	513.32	7.89 dB	50.00%	7.9999
	Peppers	466.67	7.12 dB	50.01%	7.9999
	Baboon	423.92	7.31 dB	50.00%	7.9999
	Airplane.png	501.20	7.67 dB	50.00%	7.9999
	Cameraman.png	333.42	8.22 dB	50.00%	7.9999
Petrie et al (Putrie et al., 2018)	Baboon	86.306	8.7704 dB	-	7.9989
	Airolane	10.554	7.89 dB	-	7.9928
Susanto et al (Susanto et al., 2020)	Lena	-	9.23 dB	50.02%	7.9976
	Peppers	-	8.93 dB	50.00%	7.9973
	Cameraman	-	8.39 dB	50.09%	7.9973
Arab et al (Arab et al., 2019)	Lena	-			7.9974
	Peppers				7.9972

Based on Table 2, the proposed method demonstrates superior performance in key encryption metrics compared to the studies by Petrie et al. (2018), Susanto et al. (2020), and Arab et al. (2019). Our method consistently achieves high entropy values of 7.9999 across all tested images, indicating robust encryption strength and randomness, which is slightly higher than the entropy values reported in the other studies. While our MSE values are higher, resulting in lower PSNR values, the BER remains consistently at 50%, signifying uniform encryption impact on all pixels. This is a significant advantage as it ensures that the encryption does not favor any particular part of the image, enhancing security. In comparison, Susanto et al. (2020) show higher PSNR values but with minor differences in BER and entropy. Additionally, Arab et al. (2019) provide comparable entropy values but lack detailed metrics on PSNR or BER. The comprehensive and consistent performance across all metrics in our method underscores its superior contribution to the field of image encryption, demonstrating a balanced approach between encryption robustness (high entropy) and image quality metrics (MSE and PSNR), thus proving its significant value and non-trivial advancement over the existing research.

The data shown in Figure 5 highlights the outcomes of putting both proposed algorithms into action. After thorough testing and tweaking, these algorithms were crafted to meet certain goals or tackle particular issues in their field. Figure 5 gives a clear picture, letting us see how well these algorithms perform, their strengths, and any differences between them. Essentially, it's a snapshot that demonstrates the practicality and impact of these newly developed methods.

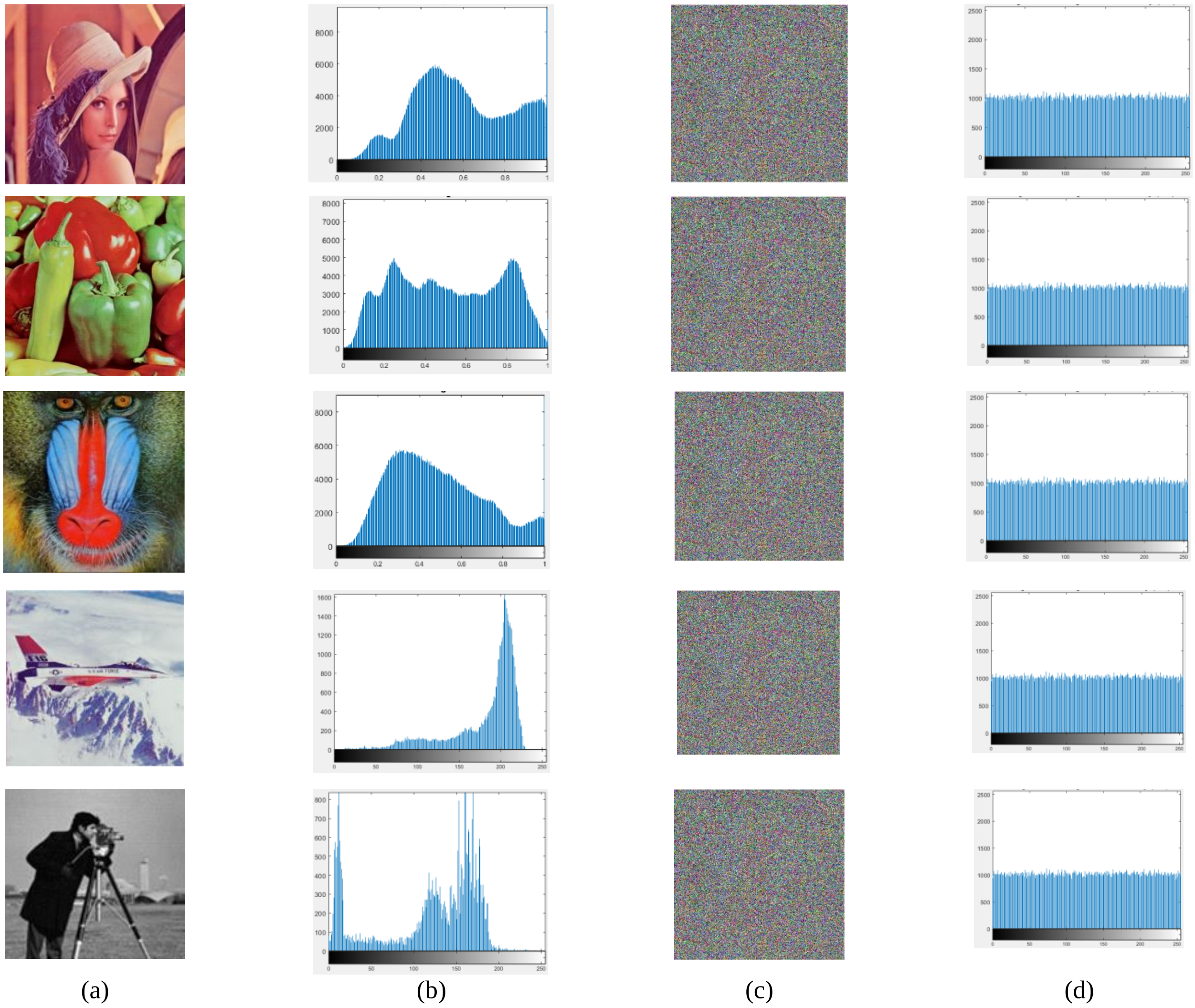
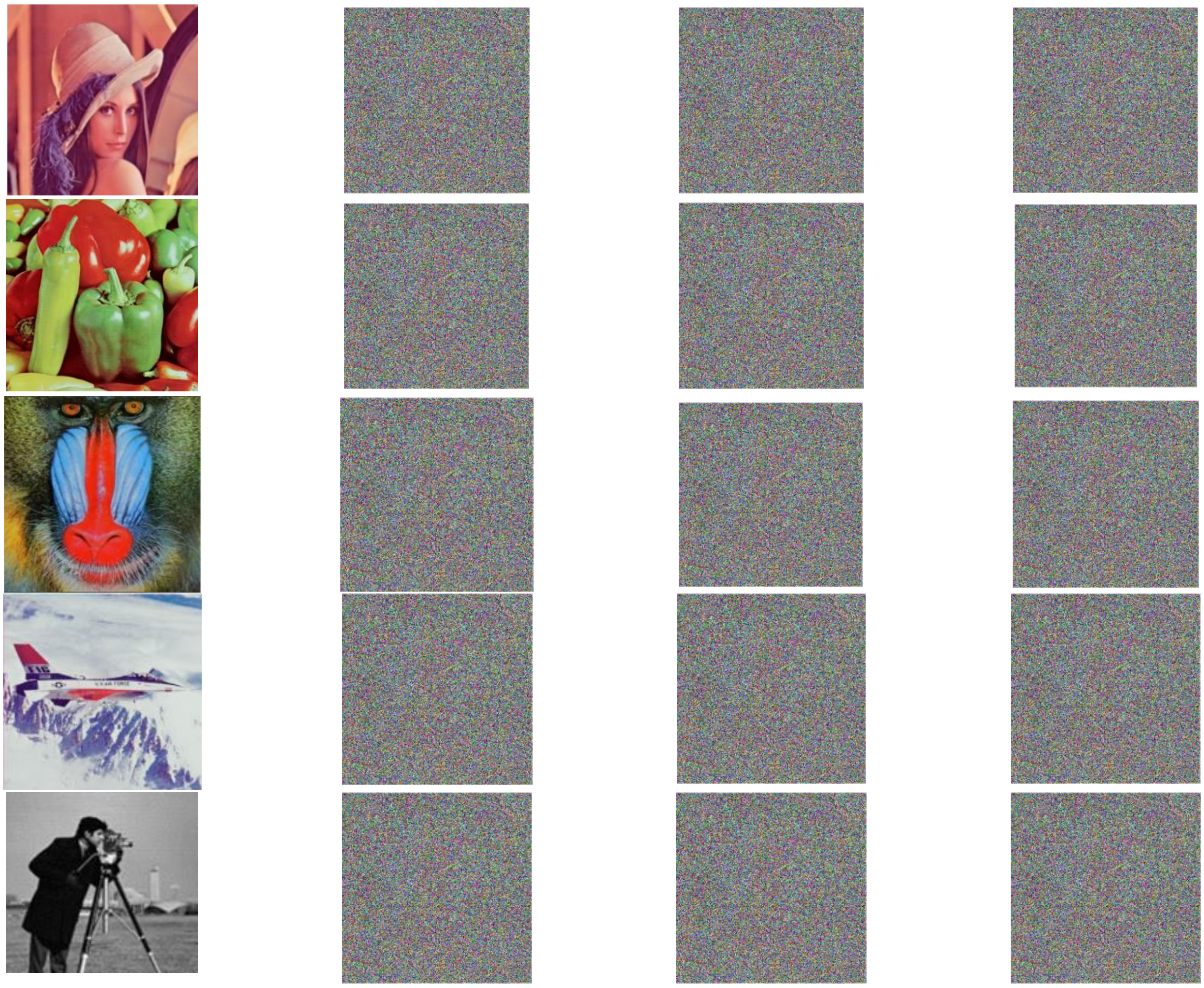


Figure 5. (a) Original Image, (b) Histogram of Original Image, (c) Encrypted Image, (d)Histogram of Encrypted Image

The results presented in Table 1 and the comparison with the proposed method demonstrate consistent MSE ranging from 333.42 to 513.32, accompanied by PSNR values between 7.12 dB and 8.22 dB across different sample images. While the proposed method maintains uniform BER at 50.00% and entropy at 7.9999, deeper analysis is warranted to ascertain the practical implications of these findings for image encryption practices. Additionally, potential challenges in real-world implementations, such as computational overhead and interoperability issues, must be addressed to ensure the viability of the proposed method in practical applications. While the proposed encryption method demonstrates uniformity in error rates and data complexity across various images, further analysis is warranted to evaluate its practical implications for image encryption practices. Specifically, the relatively low PSNR values suggest a potential trade-off between enhanced security and image quality. Moreover, the consistent BER of 50.00% highlights the need for additional measures to mitigate error propagation during the encryption process.

The sequential encryption results, executed step by step without amalgamating the related methods, are visually represented in Figure 6. This figure offers a clear and detailed depiction, illustrating each phase of the encryption process distinctly. Starting with the original 'Cover Image,' the process unfolds as it moves through the 'Columnar Transposition Encryption,' where the pixels or data undergo a strategic rearrangement based on specific rules or keys. This initial step sets the stage by adding a layer of security to the image. Building upon this, the image then enters the 'Hill Cipher Encryption' phase, using mathematical matrices and transformations to enhance its complexity and security even further. As the journey concludes, the 'Final Cipher Image (Combination)' emerges. This final product is a blend of encryption techniques, merging the organized reshuffling from the columnar transposition with the intricate mathematical adjustments from the Hill Cipher.



(a) Cover Image

(b) Columnar Transposition Encryption

(c) Hill Cipher Encryption

(d) Final Cipher Image (Combination)

Figure 6. Comparison of Encrypted Image

The comparison based on Figure 6 depicts four images: the original cover image (a), the image encrypted using columnar transposition (b), the image encrypted using Hill Cipher (c), and the final cipher image resulting from the combination of both encryption methods (d). While these images may appear visually similar, the amalgamation of these two encryption techniques provides a layered approach that enhances the overall security of the encryption process, thereby potentially thwarting unauthorized access by attackers. Furthermore, while the combination of columnar transposition and Hill Cipher offers enhanced security through multiple layers of encryption, it is essential to acknowledge potential challenges in real-world implementations. One such challenge is the computational overhead associated with applying multiple encryption algorithms, which may impact the efficiency and speed of the encryption process, especially when dealing with large volumes of image data or real-time encryption requirements.

4. Conclusion

Based on the results obtained from the combination of columnar transposition and Hill Cipher as illustrated in the provided table, several conclusions can be drawn regarding the efficacy of the encryption method. For the image 'Lena.png,' the MSE registered at 513.32, accompanied by a PSNR of 7.89 dB. Similarly, for 'Peppers.png' and 'Baboon.png,' the MSE values were 466.67 and 423.92, respectively, with corresponding PSNR values of 7.12 dB and 7.31 dB. Notably, the BER remains consistent at 50.00% across all samples, indicating a consistent error propagation rate during the encryption process. Furthermore, the entropy values for all images converge at 7.9999, suggesting uniformity in the complexity of the encrypted data. The analysis of the combined columnar transposition and Hill Cipher encryption method reveals promising consistency in error rate and data complexity, as evidenced by the uniformity in MSE, PSNR, BER, and entropy values across various image samples. However, an inclusive assessment necessitates acknowledging potential challenges and limitations in implementing the proposed recommendations. One primary concern pertains to the computational overhead incurred by integrating multiple encryption layers, which may lead to increased processing times, especially when dealing with large datasets or real-time applications. To address this, optimizing algorithms and exploring parallel processing techniques could mitigate performance bottlenecks. Additionally, the sequential layering of encryption methods might introduce compatibility issues and interoperability concerns, emphasizing the importance of rigorous testing and validation across diverse platforms. Furthermore, while the method exhibits consistency, the relatively low PSNR values suggest room for improvement in image quality and security.

For future research endeavors, an intriguing avenue to explore would be the implementation and evaluation of a three-layer super-encryption system. This advanced approach could potentially integrate multiple cryptographic techniques, such as combining columnar transposition, Hill Cipher, and another robust encryption algorithm. By layering these methods sequentially, researchers can aim to achieve an unprecedented level of security and complexity, making decryption significantly more challenging for potential adversaries. Furthermore, investigating the interplay and synergy between these distinct encryption layers could provide insights into creating more resilient and adaptive security frameworks. Such exploration would not only contribute to the advancement of encryption techniques but also address emerging challenges in data protection, particularly in sensitive sectors requiring heightened security protocols.

Acknowledgment

Thank you to the University of Dian Nuswantoro, Semarang, Indonesia for supporting this publication research.

References

[1] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, “High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD),” *Advance Sustainable Science, Engineering and Technology (ASSET)*, vol. 6, no. 1, 2024. https://doi.org/10.26877/asset.v6i1.17186

[2] V. M. Putrie, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, “Super Encryption using Transposition-Hill Cipher for Digital Color Image,” in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, IEEE, Nov. 2018, pp. 152–157. https://doi.org/10.1109/ISRITI.2018.8864361

[3] 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, 2023. https://doi.org/10.22266/ijies2023.0831.46

[4] 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. Multidisciplinary Digital Publishing Institute (MDPI), Aug. 01, 2023. https://doi.org/10.3390/computers12080160

[5] M. Abu-Faraj *et al.*, “Protecting Digital Images Using Keys Enhanced by 2D Chaotic Logistic Maps,” *Cryptography*, vol. 7, no. 2, 2023. https://doi.org/10.3390/cryptography7020020

[6] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, “A new image encryption algorithm for grey and color medical images,” *IEEE Access*, vol. 9, pp. 37855–37865, 2021. https://doi.org/10.1109/ACCESS.2021.3063237

[7] I. Prayogo Pujiono, E. Hari Rachmawanto, U. K. Abdurrahman Wahid, U. Dian Nuswantoro, and D. Anggriawan Nugroho, “The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images,” 2023.

[8] V. Kakkad, M. Patel, and M. Shah, “Biometric authentication and image encryption for image security in cloud framework,” *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019. https://doi.org/10.1007/s41939-019-00049-y

[9] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, “An efficient image encryption technique based on two-level security for internet of things,” *Multimed Tools Appl*, vol. 82, no. 4, pp. 5091–5111, Feb. 2023. https://doi.org/10.1007/s11042-022-12169-8

[10] E. J. G, H. M. A, and F. H. M. S, “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, p. 2022, 2022. https://dx.doi.org/10.14569/IJACSA.2022.01308104

[11] M. S. Abdalzaher, M. M. Fouda, and M. I. Ibrahem, “Data Privacy Preservation and Security in Smart Metering Systems,” *Energies*, vol. 15, no. 19. MDPI, Oct. 01, 2022. https://doi.org/10.3390/en15197419

[12] P. N. Lone, D. Singh, V. Stoffová, D. C. Mishra, U. H. Mir, and N. Kumar, “Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher,” *Mathematics*, vol. 10, no. 20, Oct. 2022. https://doi.org/10.3390/math10203878

[13] M. Derese Gietaneh and T. Birara Akele, “Enhancing the Hill Cipher Algorithm and Employing a One Time Pad Key Generation Technique,” *Abyssinia Journal of Engineering and Computing Abyss. J. Engg & Comput*, vol. 3, no. 1, pp. 1–10, 2023.

[14] H. N. Khalid, A. Hafizah, and M. Aman, “Digital Image Steganography in Spatial Domain: A Critical Study,” 2020.

[15] S. Gupta, K. Saluja, V. Solanki, K. Kaur, P. Singla, and M. Shahid, “Efficient methods for digital image watermarking and information embedding,” *Measurement: Sensors*, vol. 24, p. 100520, Dec. 2022. https://doi.org/10.1016/j.measen.2022.100521

[16] M. Fadlan, Haryansyah, and Rosmini, “Three Layer Encryption Protocol: an Approach of Super Encryption Algorithm,” in *2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, Oct. 2021, pp. 1–5. https://doi.org/10.1109/ICORIS52787.2021.9649574

[17] M. A. Budiman, Amalia, and N. I. Chayanie, “An Implementation of RC4+ Algorithm and Zig-zag Algorithm in a Super Encryption Scheme for Text Security,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Mar. 2018. https://doi.org/10.1088/1742-6596/978/1/012086

[18] C. Umam, L. B. Handoko, C. A. Sari, E. H. Rachmawanto, and L. A. R. Hakim, “Kombinasi Vigenere dan Autokey Cipher dalam Proses Proteksi SMS Berbasis Android,” *Prosiding Sains Nasional dan Teknologi*, vol. 12, no. 1, p. 492, Nov. 2022. http://dx.doi.org/10.36499/psnst.v12i1.7108

[19] 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. https://doi.org/10.4236/jcc.2019.73002

[20] D. E. Mfungo and X. Fu, “Fractal-Based Hybrid Cryptosystem: Enhancing Image Encryption with RSA, Homomorphic Encryption, and Chaotic Maps,” *Entropy*, vol. 25, no. 11, p. 1478, Oct. 2023. https://doi.org/10.3390/e25111478

[21] B. Zolfaghari and T. Koshiba, “Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap,” *Applied System Innovation*, vol. 5, no. 3. MDPI, Jun. 01, 2022. https://doi.org/10.3390/asi5030057

[22] M. Kaur, S. Singh, and M. Kaur, “Computational Image Encryption Techniques: A Comprehensive Review,” *Mathematical Problems in Engineering*, vol. 2021. Hindawi Limited, 2021. https://doi.org/10.1155/2021/5012496

[23] J. Gao, Y. Wang, Z. Song, and S. Wang, “Quantum Image Encryption Based on Quantum DNA Codec and Pixel-Level Scrambling,” *Entropy*, vol. 25, no. 6, Jun. 2023. https://doi.org/10.3390/e25060865

[24] A. Susanto *et al.*, “Triple layer image security using bit-shift, chaos, and stream encryption,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 980–987, Jun. 2020. https://doi.org/10.11591/eei.v9i3.2001

[25] A. Arab, M. J. Rostami, and B. Ghavami, “An image encryption method based on chaos system and AES algorithm,” *Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, Oct. 2019. https://doi.org/10.1007/s11227-019-02878-7