AI-Driven Cryptographic and Steganographic Integration for Enhanced Text Security Using OpenAI API

Omar Fitian Rashid[1,*], Saba A. Tuama[2], Imad J. Mohammed[1], Mohammed Ahmed Subhi[3]

[1] Department of Geology, College of Science, University of Baghdad, Baghdad, Iraq

[2] Department of Engineering, University of Information Technology and Communications, Baghdad, Iraq

[3] Department of Planning, Directorate of Private University Education, Ministry of Higher Education and Scientific Research, Baghdad, Iraq

Emails: omar.f@sc.uobaghdad.edu.iq; saba.ayad@uoitc.edu.iq; emad.j@sc.uobaghdad.edu.iq; mohammed-ahmed@mtu.edu.iq

Abstract

Artificial Intelligence (AI) can become a great asset to produce cryptographic keys in order to improve the security of the encryption methods. While using machine learning algorithms AI can generate most complex and unpredictable keys to prevent brute-force and cryptanalyst attacks. Key generation using AI also allows the design of cryptographic solutions that adapt to the context in which the key is used. It also enhances the conventional security measures while simultaneously providing great opportunities for creating flexible security solutions. This paper proposed a new text security method based on the integration of the cryptography and steganography, where the suggested method is done based on OpenAI API. The proposed method is consisted of three steps, and these steps are key generation, text encryption, and data embedding. The first step, is utilized by using GPT-2 model to generate set of keys for both cryptography and steganography steps. The second step, is starting by converting the plaintext to ASCII format, then performed modulo arithmetic operation between ASCII values and the keys that generated from the previous step, then convert the achieved equation results to Hexadecimal format, and finally convert these values to binary and these values represent the final ciphertext. The last step of the proposed method is done by hiding the binary values within image, this done by select positions randomly, then used GPT-2 model to generate another set of keys to shift the values of random positions, then applied least significant bit (LSB) algorithm to hide the bits within the final position with different color channels. The proposed approach provides a basis for the development of new-generation secure communication systems in the context of AI.

Keywords: Cryptography; Artificial intelligence; Steganography; ChatGPT; Encoding

1. Introduction

Artificial intelligence is a new branch of computer science where a human or a computer program teaches a computer how to think like a human being. By using machine learning, natural language processing and neural networks AI systems can deal with massive amount of data and identify patterns, make decision and execute tasks on their own [1-2]. On other hand, security can define as the measures and procedures aimed to protect computer systems, data, and networks from unauthorized access, theft, damage or interference [3]. Where security is an essential component of today has developed digital environment, covering hazards from cybercriminals, info leakage, and system weaknesses. With the growth of smart attacks, security measures have become preventive and encompass threat identification, encryption as well as intrusion prevention [4]. AI and security are two interrelated fields meaning that the two borrow and develop from each other. AI improves security because threats can be detected and analysed in real-time with the subsequent possibility to counteract them together with such threats as high-impact cyberattacks. They can work through large amount of data, to identify occurrences of security breaches, analyse signs of such breaches, and learn about new types of threats. On the other hand, security of these AI technologies is paramount since these technologies

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

can be attacked via data poisoning, adversarial inputs and model theft. Integrated between AI and security is paramount for dealing with issues within the context of a dynamic technological environment, in which AI creates new security solutions while at the same time the security field guarantees the stability and credibility of AI solutions. Combined they offer a framework for constructing robust, flexible, and safe systems in a world that is increasingly interconnected [5-6].

A large number of cryptographic techniques has been proposed and published in the literature over the years, where different methods have been suggested by researchers to deal with numerous security issues and strengthen security. A new visual cryptography method is proposed by [7], where the suggested method is starting by fusion both cover and hidden images based on advanced data embedding techniques. Then, divided image into 3 × 3 blocks, then used a secret key for encryption the picture. Francis and Monoth [8] presented a new random visual cryptography, this done by using multiple security layers with embedding method, where the main advantage is the pixel expansion and codebook design issues are averted. A novel method to enhance the security database based on cryptography and genetic operators is proposed [9], where this method starting with data encrypting based on cryptographic algorithms. After that, applied the genetic operators for encryption process enhancement. A new cryptography method is suggested to encrypt the sensitive data [10], this method is done by using privacy score value to isolated sensitive attribute from non-sensitive attributes, and then generated set of keys, and finally, adaptive elliptical curve cryptography method is applied. Sharma et al. [11] proposed a new text cryptography method based on elliptic curve cryptography, where this method is done by leveraging elliptic curve coordinates as keys. An image encryption method is suggested by [12] based on elliptic curve cryptography (ECC) method. Firstly, ECC is applied to encrypt image, then shuffled the rows and columns for the cipher-image. Saravanaselvan and Paramasivan [13] suggested a new One-Time pad cryptographic method based on Huffman Source Coding with Energy Aware sensor node Design, where the distance needs for sending is calculated before transmission with the using of WSN applications. Various existing security vulnerabilities was analyzed by [14], and then proposed corresponding security suggestions and improvement measures for authentication schemes identification and carry out security evaluation of cryptographic algorithms. A novel cryptography method is suggested based on Neural Networks Graph and machine learning to classify Bitcoin transactions either illicit or licit [15], where the suggested method is done using Elliptic dataset data. Shidaganti et al. [16] proposed a new security method in cloud based on both cryptography and image steganography, this done bay using Advanced Encryption Standard method and Diffie-Hellman algorithm. A hybrid cryptography method is built to enhance cloud security based on symmetric and asymmetric encryption methods [17], where AES method is applied at the sender's side, while the ECC method is applied at the receiver side.

Due to patterns and randomness, AI model generating keys are more complex and resistant to hacking and cryptanalysts. This approach also allows the output keys to be developed and updated more rapidly while enhancing the general protection of data. The main contributions of the proposed system are:

- Advanced Key Generation: AI-embedded GPT-2 is used for cryptographic and steganographic keys generation, thus increasing the complexity and non-linearity of the used security aspects.
- Integrated Cryptography and Steganography: Applies both cryptographic encryption and steganography to come up with a two-tier principle of security in communication.
- Context-Adaptive Security: Optimizes adaptations of cryptographic solutions with regard to key usage scenarios, enhancing flexibility of usage in various situations.
- Steganographic Innovation with AI: Integrates GPT-2-produced keys for elements of data embedding location in images, increasing steganography operations' security and unpredictability.
- Foundation for AI-Based Security Systems: Creates a new paradigm for incorporating AI into cryptographic and steganographic techniques for building the future generation of secure communication systems.

The paper is organized as follows: section 2 clarifies the materials and methods of the proposed method. Then, in section 3, the evaluation criteria and the achieved results of the proposed method is presented. Finally, the conclusions are described in section 4.

2. Materials and Methods

A new security method is developed by using GPT-2 to generate encryption keys and employing steganography for image embedding. Where the proposed method methodology is divided into three steps: key generation, text encryption, and data embedding, where the steps of the proposed method is shown in Figure 1

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

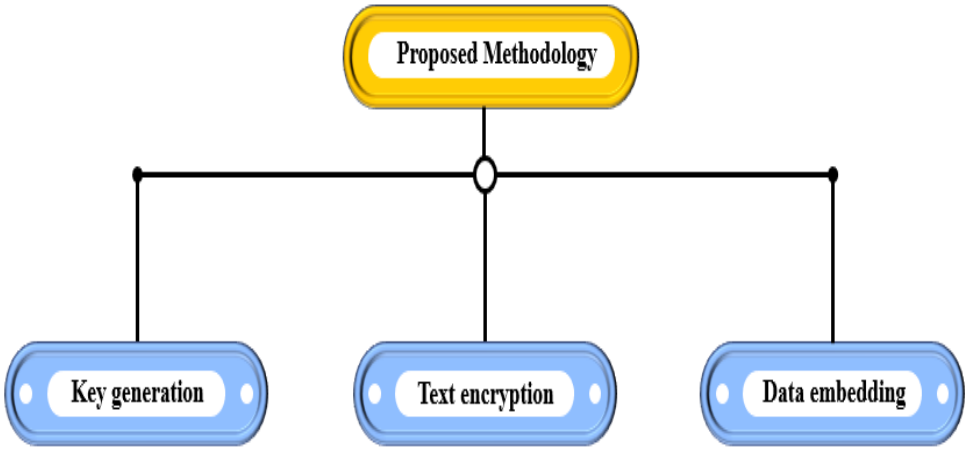

Figure 1. The steps of the proposed methods

A. Key Generation Using GPT-2

The first step is creating encryption keys based on the GPT-2 model, where GPT-2 is used due to its generative language model with high language generation capacity derived from the input prompt, and it used to create set of encryption keys that will be more secure. Where a special call is made to guide GPT-2 to create a random cryptographic key and the call itself is created to ensure that the resulting key is truly random. For example, the model can be prompted with: "write out secure sets of encryption keys in decimal form".

B. Text Encryption

The second step of the proposed method is text encryption, this method is done to encrypt the plaintext message using five steps and these steps are shown in Figure 2.

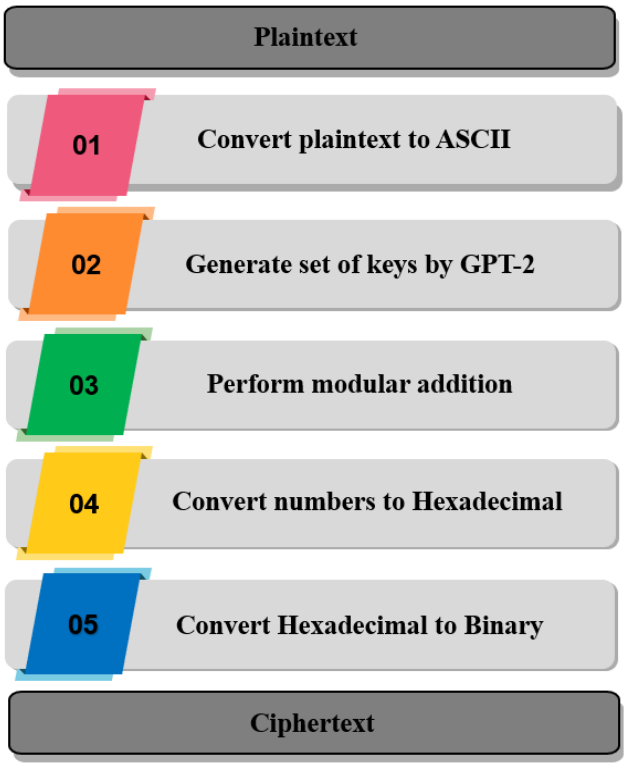

Figure 2. The steps of the proposed methods

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

As shown in Figure 2, the proposed cryptography method is starting by converting the plaintext characters to numerical form using a character to code conversion (ASCII) where each character is converted to its equivalent ASCII value, then a simple modulo arithmetic is performed on the textual data using the key which helps to ensure that the encrypted text is just sufficiently non-linear yet is not computationally expensive, and this done based on the following equation

$$Enc = (Plaintext\ character\ (in\ ASCII) + first\ number\ from\ generated\ key)\ mod\ 256 \quad (1)$$

After that, the encrypted output is encoded to another format (hexadecimal string), and finally, the obtained hexadecimal string is converted to binary format and these numbers are represent the final ciphertext to embedded with the cover image. The proposed cryptography steps are clarified in Algorithm 1.

Algorithm 1: Cryptography

Input: Plaintext

Output: Ciphertext

Step 1. Plaintext Converting to ASCII

Convert each character within plaintext to its equivalent ASCII format.

Step 2. Key generation

Use OpenAI GPT-2 to generate a cryptographic key (include set of keys).

Step 3. Perform modular addition

Apply the following equation for each character in plaintext

character in ASCII + generated key = the total (mod 256)

for example: O (79) + 127 = 206 (mod 256) = 206

Step 4. Results converting to Hexadecimal

Convert each achieve results to its equivalent Hexadecimal format.

Step 5. Hexadecimal converting to Binary

Convert each Hexadecimal to binary, and the achieved numbers are representing the ciphertext.

Step 6. End encryption:

Return the ciphertext.

End Algorithm

C. Data Embedding within Image

Finally, after converting the text into machine code is followed by steganography where the encrypted text is integrated into an image based on the steps that illustrated in Figure 3.

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

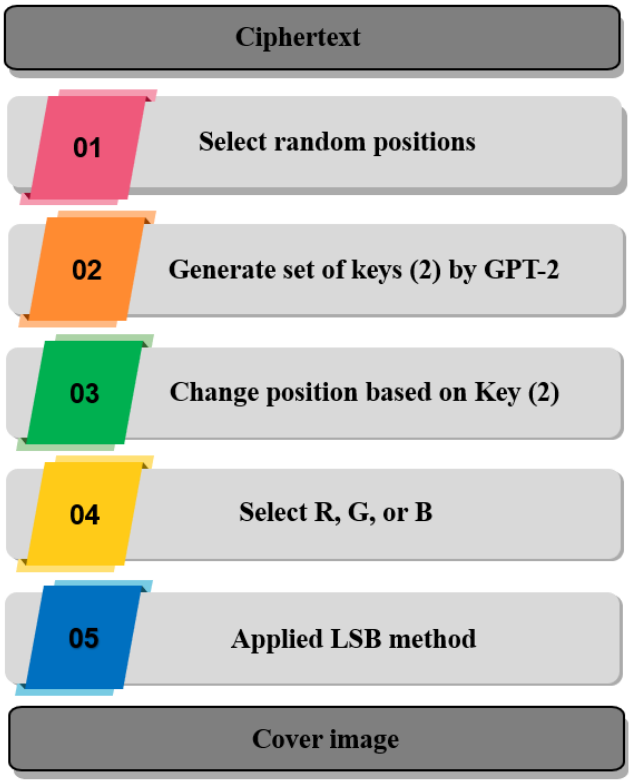

Figure 3. The proposed steganography steps

Where the used image is function as the carrier (cover image) and must be able to hold enough capacity for the encrypted data. For this purpose, select random positions within image (select random X and Y values), then GPT-2 model is used to generate set of keys to shift the selected positions based on these keys, the LSB method is used because of the easy implementation and does not disrupt the visual quality. The LSB is applied within image pixels, and each pixel are made of 3 color channels (Red, Green Blue) and the least significant bit of each of the 3 colors is change, where the color channels is also chosen randomly. The same process is done until all the binary data will be inserted in the cover image, and finally saving the Stego-Image and can send it securely. The proposed steganography steps are clarified in Algorithm 2.

Algorithm 2: Steganography

Input: Ciphertext (in binary)

Output: Cover image

Step 1. Load ciphertext and the Image

Load the achieved binary sequences that achieved from Algorithm 1 as ciphertext, and load the image to hide the message inside it.

Step 2. Select hiding positions

After choose the image, based on their height a width we choose random X and Y positions.

Step 3. Key generation

Use OpenAI GPT-2 to generate a key to shift selected position that obtained from previous step (include set of keys).

Step 4. Choose the pixel's Color embedded

Select either to embedded the binary number in red or green or blue.

Step 5. Application of Least Significant Bit method

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

Applied least significant bit (LSB) of each pixel in the image to embed the binary sequence in one color channel.

Step 6. End message hiding:

Return the cover image.

End Algorithm

3. Results and Discussions

The performance evaluation of the suggested method is done based on calculation the cryptography and steganography times, where Table 1 and Figure 4 are shown the encryption and decryption times needed to converted plaintext to ciphertext and vice versa, this done by using different messages with various sizes.

Table 1: The required cryptography times in term of seconds

Message size (characters)	Encryption (s)	Decryption (s)
100	0.041	0.018
500	0.236	0.114
1000	0.483	0.374
1500	0.710	0.424
2000	0.862	0.503
2500	1.379	0.918
5000	1.986	1.56
10000	4.025	2.78

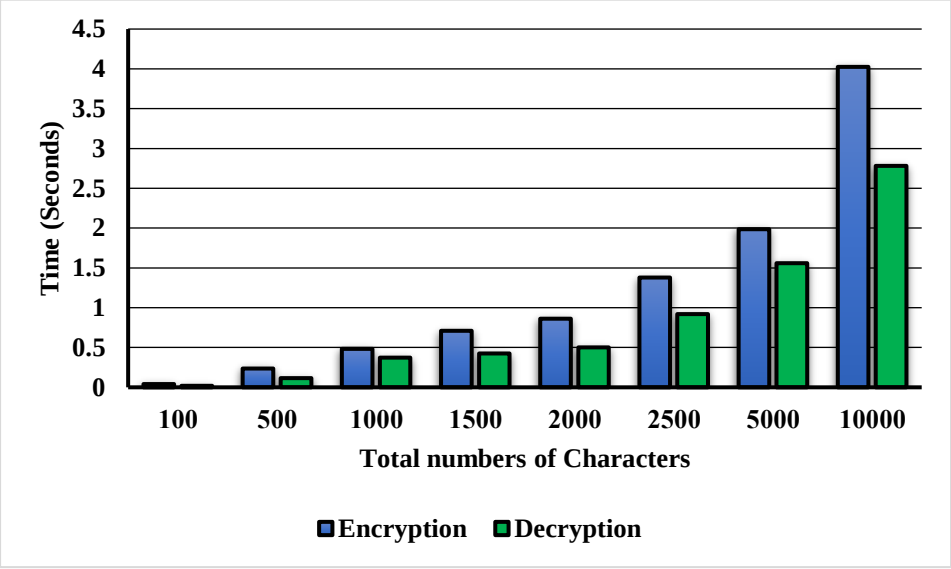

Figure 4. The required cryptography times in term of seconds

While the bits hiding and restoring times required to embedded and extracted ciphertext within image by using different messages with various sizes are shown in Table 2 and Figure 5.

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

Table 2: The required steganography times in term of seconds

Message size (characters)	Hide (s)	Extract (s)
100	0.034	0.007
500	0.187	0.049
1000	0.313	0.154
1500	0.499	0.266
2000	0.580	0.402
2500	0.632	0.479
5000	1.159	1.002
10000	2.603	1.879

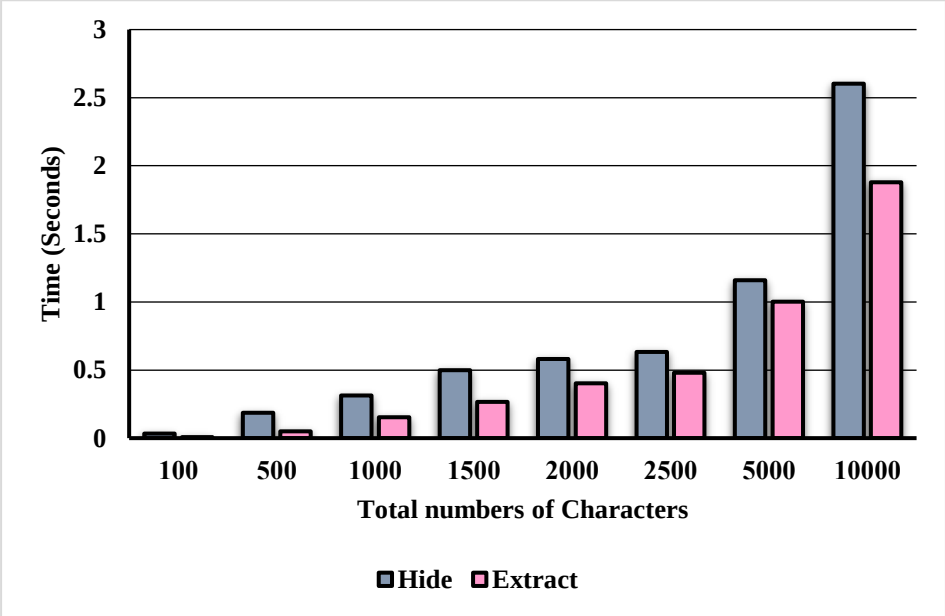

Figure 5. The required steganography times in term of seconds

4. Conclusion

This study is proposed a new text security method using both cryptography and steganography; the suggested method is depending on the concept of AI. Integrating the keys generated by GPT-2 with the LSB and using an efficient steganographic approach for concealing, this methodology offers a new and secure model for text encryption. Randomness of GPT-2 model along with the characteristics of steganography guarantees the encrypted text's safety and its impossibility to read by intruders. For future work, investigate the improvement of the current technique to the more sophisticated GPT-4, and can expand the encrypted text capability to other more formats, audio, video, and 3D models.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

References

[1] B. Sharma, P. Goel, and J. K. Grewal, "Advances and Challenges in Cryptography using Artificial Intelligence," *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*, Lonavla, India, pp. 1–5, 2023. doi: 10.1109/I2CT57861.2023.10126338.

[2] O. Ahmed, "Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration," *International Journal of Mathematics, Statistics, and Computer Science*, vol. 2, pp. 244–258, 2024. doi: 10.59543/ijmscs.v2i.10377.

[3] O. F. Rashid, Z. A. Othman, and S. Zainudin, "Features Selection for Intrusion Detection System Based on DNA Encoding," in *Intelligent and Interactive Computing*, V. Piuri, V. Balas, S. Borah, and S. Syed Ahmad, Eds., *Lecture Notes in Networks and Systems*, vol. 67, Singapore: Springer, 2019. doi: 10.1007/978-981-13-6031-2_23.

[4] T. Nathiya, B. Mahalakshmi, K. K. Savitha, S. Pal, A. A. Khan, and R. Kumar, "A Comprehensive Approach to Cryptography and Security Testing in Network Defence," *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, Windhoek, Namibia, pp. 1–6, 2024. doi: 10.1109/ETNCC63262.2024.10767436.

[5] P. Kumar, A. Laroia, M. Kumar, A. Laroia, K. Upreti, and J. Parashar, "Advancing Image Security Through Deep Learning and Cryptography in Healthcare and Industry," *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, Windhoek, Namibia, pp. 236–441, 2024. doi: 10.1109/ETNCC63262.2024.10767450.

[6] G. I. Loretta, I. Kasireddy, M. Prameela, D. S. N. M. Rao, M. Kalaiyarasi, and S. Saravanan, "Enhancing Network Security with Multifused Cryptography: Integrating IoT and AI," *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, pp. 1–6, 2024. doi: 10.1109/ICDSNS62112.2024.10690933.

[7] N. M. Sultana and K. Srinivas, "Data Privacy Protection in Cloud Computing Using Visual Cryptography," *Multimedia Tools and Applications*, 2024. doi: 10.1007/s11042-024-19963-6.

[8] N. Francis and T. Monoth, "Security enhanced random grid visual cryptography scheme using master share and embedding method," *International Journal of Information Technology*, vol. 15, pp. 3949–3955, 2023. doi: 10.1007/s41870-023-01381-w.

[9] S. R. Devara and C. Azad, "Improved Database Security Using Cryptography with Genetic Operators," *SN Computer Science*, vol. 4, p. 570, 2023. doi: 10.1007/s42979-023-01990-z.

[10] S. Vinothkumar and J. Amutharaj, "A hybrid public cryptography-based group key generation for sensitive attribute protection in medical healthcare systems," *International Journal of Information Technology*, 2024. doi: 10.1007/s41870-024-02306-x.

[11] P. L. Sharma, S. Gupta, H. Monga, A. Nayyar, K. Gupta, and A. K. Sharma, "TEXCEL: Text encryption with elliptic curve cryptography for enhanced security," *Multimedia Tools and Applications*, 2024. doi: 10.1007/s11042-024-19377-4.

[12] I. Chaouch, A. Naanaa, and S. ElAsmi, "A hybrid scheme using hyper-chaotic system and elliptic curve cryptography for image encryption," *Multimedia Tools and Applications*, 2024. doi: 10.1007/s11042-024-19173-0.

[13] A. Saravanaselvan and B. Paramasivan, "A one-time pad cryptographic algorithm with Huffman Source Coding based energy-aware sensor node design," *Sustainable Computing: Informatics and Systems*, vol. 44, 2024. doi: 10.1016/j.suscom.2024.101048.

[14] L. Zhang, J. Sheng, Y. Zhang, and Q. Wu, "Evaluation of Cryptography Algorithm Based on Digital Identity Authentication," *Procedia Computer Science*, vol. 247, pp. 1012–1019, 2024. doi: 10.1016/j.procs.2024.10.122.

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025

[15] Y. N. Kiran and N. Bala, "Enhancing Elliptic Curve Cryptography with Graph Neural Networks and Ensemble Methods," *2024 9th International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, Okinawa, Japan, pp. 837–840, 2024. doi: 10.1109/ICIIBMS62405.2024.10792850.

[16] G. Shidaganti, V. L. Manoj, M. Vinay, and P. Patil, "Enhancing Data Protection Using Cryptography and Image Steganography in Cloud Environment," *2024 5th International Conference on Circuits, Control, Communication and Computing (I4C)*, Bangalore, India, pp. 93–99, 2024. doi: 10.1109/I4C62240.2024.10748507.

[17] A. Tiwari, A. K. Pandey, L. Singh, G. K. Tiwari, and A. Singh, "Hybrid Cryptography Algorithms for Cloud Data Security," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, pp. 1–5, 2024. doi: 10.1109/ICCCNT61001.2024.10725233.

DOI: https://doi.org/10.54216/FPA.190110
Received: November 24, 2024 Revised: January 23, 2025 Accepted: February 17, 2025