



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

A Lightweight Image Encryption Algorithm Based on Secure Key Generation

Sumit R. Gore^{1*}, Dr. Pragati Patil², Prof. Anita Yadav³, Prof. Poonam Bhamburkar⁴

¹ M.Tech Research Scholar, Department of Computer Science and Engineering, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, Maharashtra, India. Email: sumitgore1997@gmail.com

² Vice Principal, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, Maharashtra, India. Email: viceprincipal@tgpcet.com

³ Head, Department of Computer Science and Engineering, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, Maharashtra, India. Email: hod.cse@tgpcet.com

⁴ Department of Computer Science and Engineering, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, Maharashtra, India. Email: poonam.cse@tgpcet.com

*Corresponding author: Sumit R. Gore (sumitgore1997@gmail.com)

Abstract

The explosive increase in the transmission of digital images and cloud-based storage has made confidentiality and integrity of visual data an important security requirement. Image encryption is an important tool for protecting sensitive information from unauthorized access and cyber threats. In this paper, we propose full image encryption and decryption framework based on the AES which is implemented from scratch without using any external cryptographic libraries. The system takes any digital image as input. The system converts pixel level data into secure binary cipher text by using AES symmetric key cryptography. The information of the image becomes incomprehensible to the binary data by the encryption process and can not be used for visual and statistical inference attacks. The encrypted output is stored in a special repository and cannot be viewed or re-created without the proper decryption process. During decryption, the same AES key and algorithmic structure are used to reprocess the encrypted binary data, restoring the original image without loss of quality. The framework supports flexible image formats and shows the reliable reversibility, confidentiality and robustness to unauthorized access. This system integrates the encryption and decryption into a single application flow for the purpose of computational efficiency and secure image handling. The approach demonstrates the usefulness of AES in multimedia security applications, especially in the context of secure image storage, transmission and access control.

Keywords: Image encryption, Advanced Encryption Standard, symmetric cryptography, binary cipher data, secure image transmission, data confidentiality, cryptographic security, image decryption."

1. Introduction

The rapid evolution of digital technologies has resulted in a significant growth in the generation, transfer and storage of image data on network and cloud platforms and connected devices. There are many types of sensitive and private data contained in images, including personal identity, medical details, video footage captured by cameras, manufacturing process information, etc. As unauthorized access, tampering or leakage of such images can lead to privacy violations, financial losses and compromised decision-making [1], the security of such images has become increasingly important. Common protection methods like password authentication and basic encryption are not sufficient to resist sensitive image interception, visual analysis and statistical attacks in the present-day cyber environment [2].

Cryptographic techniques have been proven to be a reliable solution to secure digital images, which can offer confidential, controlled and integral access. Among these, symmetric key cryptography is widely popular, because of its efficiency and security properties [3]. Image encryption is the process of transforming the information in the image into a meaningless form, that would not be understandable without the key, but would be perfectly readable when required [4]. The Advanced Encryption Standard has been growing in popularity as the preferred choice to secure images because it has the capacity to encrypt a vast amount of data with a high level of robustness against cryptanalysis [5]. AES is a pixel level encryption in which the content of the image cannot be deduced visually or statistically from the stored or transmitted image [6].

In recent years, it has been demonstrated that AES can be used in a variety of applications such as hybrid encryption schemes, chaotic key integration and edge-computing scenarios [7]. The methods enhance the security by using AES and other methods, which enable the generation of dynamic keys, efficient processing and secure image transmission on various platforms [8]. AES-based encryption can also be incorporated with cloud storage and IoT systems, maintaining confidentiality without affecting the performance [9]. It

can be used in real time and multi format environments highlighting its versatility and robustness in the secure handling of images [10].

The purpose of this work is to develop an application that is able to secure images through encryption and decryption processes with the AES developed from first principles. The system is capable of encrypting any image into binary data, so that no one can access it. Later on the system is able to decrypt the image and restore it exactly as it was. The framework enables a user-friendly interface for handling uploading, encryption, storage, decryption, and assuring the confidentiality, integrity and controlled access to sensitive visual data.

2. Related Work

The C-HIDE Steg is a hybrid image encryption algorithm based on AES and ECC that is presented by El-Rahman et al. [11] without using cover image. Highly secure and strong data hiding technique. The images can be secured from interception, tempering, and unauthorised access, without visually change to the original image. The AES with ECC enhances key management capabilities and provides strong cryptographic security, making it an ideal solution for sensitive applications like confidential communications and cloud-based storage systems. In the research by Gondowarsito [12] was studied encryption and decryption of multi-format data with AES algorithm (cipher block chaining) using the programming language Python. The study demonstrated that AES could be used with different image and file formats, maintaining data integrity and confidentiality under various storage and processing environments. The work highlighted the need of block based transformations and secure chaining mechanism to avoid pattern recognition attack and extraction of information on the image by unauthorized parties.

Liu et al. [13] proposed an image encryption algorithm by HNN based processing using memristor. Using this approach, high security can be obtained, as it adds nonlinearity and dynamics to the encryption process, which make the data securely protected at the pixel level, and makes the data unreconstructable without permission. This approach showed the potential to combine the intelligence of the neural network with hardware level innovation to enhance the efficiency and robustness of the encryption. Husam et al. [14] proposed a hybrid encrypted algorithm of DES and present algorithm using 2D chaotic system for color image encryption. The chaotic maps added to the randomness and statistical attack resistance. The hybrid combination of DES and Present ensures the layered security. The results showed the importance of hybrid cryptographic techniques for the protection of images against advanced attacks.

In [15] Sihwail and Ibrahim proposed a new image encryption algorithm using optimized smart codebook. The approach aimed to reduce the computational complexity and maintain high security levels. The codebook based transformation ensured the shuffling and substitution of the patterns in the encrypted image were done appropriately so that the patterns are not visible that way. This work put forward the efficiency and scalability as significant aspects in modern image security systems. Wandile et al. [16] proposed a compact and secure image encryption scheme for IoT applications based on a hybrid AES and ECC cryptography. The research was aimed at lightweight encryption of resource constrained device, which had strong security. They achieved secure image transmission in IoT networks while not degrading the performance, using ECC for key management and AES for bulk image encryption.

You can use a memristor-based hyperchaotic hybrid encryption scheme to encrypt images on a Jetson TX2 platform with DNA-based encoding, as designed by Ulutas [17]. The system was based on hyperchaotic sequences that shuffled the pixels, and DNA encoding for the substitution, offering a very high level of security. In this work, a real-time protection scheme for image data using unconventional cryptographic techniques with hardware accelerators were demonstrated. Saini and Sehrawat [18] have introduced a CNN-AES system for image block encryption using multi-key approach. The approach was to segment the images into blocks and apply convolutional neural networks to enhance the encryption diffusion and then the image was safely encoded using AES with multiple keys. The resistance against differential attacks is increased and a secure block-level image handling is provided by this approach.

In [19] Vayadande has studied the hybrid approach of symmetric and asymmetric cryptography for image encryption and decryption. The research revealed that hybrids systems were more secure than stand alone systems, and they not only facilitated efficient key exchange but also efficient bulk encryption. Flexibility to various image formats and dynamics were highlighted in the study. Maiti et al., [20] did the comparison of asymmetric key cryptographic algorithms for image encryption and discussed the performance and security of various methods. The study revealed the trade-offs of the strength of encryption, computation complexity and applicability for different image sizes. Optimization of security requirements, performance restrictions and application fields were highlighted to select the suitable algorithm. The papers presented in this conference demonstrate the current development of image encryption techniques and highlight hybrid methods, chaotic systems, integration of neural networks and hardware-assisted methods. They strengthen the need for AES based frameworks and complementary algorithms to provide strong, efficient and versatile security for image data across various platforms and environments. The content of these works could serve as a basis for the development of more sophisticated image encryption systems which

can cope with the more contemporary confidentiality and integrity requirements in digital image communication and storage.

3. Materials And Methods

This proposed system will be used for secure image encryption and decryption application with advanced encryption standard. The system is intended to protect the digital image on a pixel-level. It makes it possible for the user to upload any image and it is converted into binary encrypted data which makes visual content confidential and not accessible to unauthorized parties [21]. The system enables safe storage of encrypted images and their re-upload for controlled decryption, without losing image quality and data, and correctly restoring the original image [22]. The application features a user-friendly interface to simplify the image upload, encryption, storage and decryption processes, offering a seamless and reliable environment for secure image handling. The system additionally secures against information leaks, tampering, and unauthorized access by converting pictures into non-viewable encrypted information, which makes it appropriate for sensitive applications like cloud storage, medical imaging, and electronic archives [23]. The strategy is focused on data integrity, privacy and controlled access.

Fig. 1. System architecture for AES Image Encryption & Decryption Application. This is a user uploading any plain image for AES Encryption Process or Encrypted image for AES Decryption Process. The contents of the workflow will be encrypted in binary (BCD) format and securely stored as encrypted image files in a special folder.

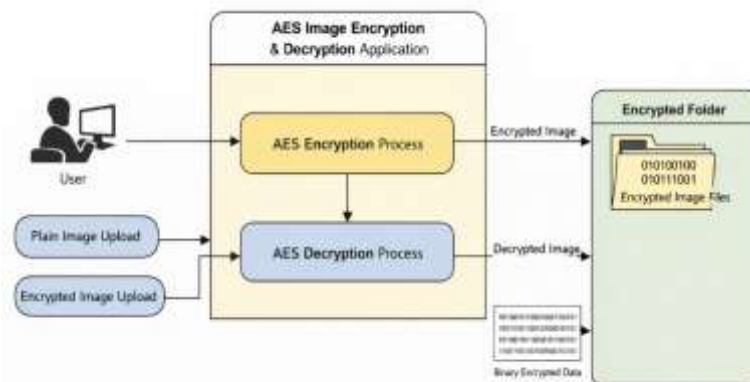


Fig.1 Proposed Architecture

Step 1. Choose and upload a digital photo to the app. The user can select images in JPEG, PNG or BMP format providing them with a flexibility of use for various applications. Once an image is uploaded, the system verifies the integrity of the image, and displays a preview of the image to ensure that the image has been selected for encryption. The image performs some preprocessing for making the image uniform for encryption. This requires resizing (if needed) to fit the processing power of the encryption module and a conversion to a standard color space, typically RGB. The pixel values are then read off and saved in a matrix or array. This is the initial data given as input to the encryption algorithm. Preprocessing also involves checking the image for any corruption or incompleteness of the data that can cause errors in the encryption process. The image preparation allows the methodology to execute all the subsequent encryption operations efficiently without compromising the accuracy of the data and easily integrates into the encryption workflow. This is one of the important steps to ensure that the quality and integrity are maintained throughout the process.

i) Image Upload and Preprocessing: After upload and pre-processing, the image is encrypted, and the readable information of the image is transformed into an unviewable form. In this workflow the pixel matrix is read and processed in blocks, yielding a uniform application of the security. Each block of pixels is encrypted into binary data in a systematic way. In the encryption process, the security is increased by several layers of operations such as substitution, permutation and mixing of pixel information to prevent the reconstruction of the original image by unauthorized users even if the encrypted file is intercepted. The binary data of the image is then embedded into a specific folder or database in a specific format, which means that it is encrypted. More metadata can be included for integrity control, like file size or checksum, to ensure that it can be retrieved accurately when decrypting. This workflow results in a very secure image, as it is protected at the pixel level, and is resistant to statistical attacks, visual analysis or pattern detection, but allows for later decryption if the proper key is used.

ii) Image Encryption Workflow: This method lets the user upload the encrypted image to a server after the image was encrypted to decrypt and verify it. The system performs integrity checking of the encrypted file that was uploaded to ensure that the uploaded file was not corrupted or changed since it was uploaded.

Validation is to verify the binary structure, file size, etc. any other metadata. This is to make sure that the image can be decrypted properly. This step helps to avoid any loss or errors in the data during decryption. Once the validation is done, the encrypted data is loaded into memory in the form of a matrix of binary values. This is the encrypted picture representation. The system then matches this data with the original encryption parameters such as block size, key length and the sequence of operations used during encryption to set it up for decryption. With the help of this technique, it is possible to greatly manage security and control who has the right to access the confidential information contained in the image: the image is consistent, the privacy is guaranteed and it can be processed securely and accurately to be restored.

iii) Encrypted Image Upload and Validation: The decryption process is the opposite of the encryption process, and is used to find the image from the encrypted binary data. Once the valid encrypted image has been loaded, the decryption algorithm is used. Key and block used as in the encryption step. The binary data is then systematically passed through several inverse operations (inverse permutation, substitution and transformation), to recover the original pixel values. This ensures that the resulting image looks like the input image in terms of colour, resolution and integrity of the image itself. The decrypted image is then shown to the user for confirmation, and can be optionally saved in a secure folder. The method can ensure high accuracy of the decryption process, and can also keep the image quality, so that there is no data corruption or visual distortion. In addition, error checking mechanisms can maintain the uniformity of the restored and original images to provide safe access to visual information. This workflow demonstrates the controlled access, confidentiality and safe processing of images in the entire encryption-decryption cycle.

iv) Image Decryption Workflow: Uploaded images are encrypted with a well-known and robust cryptographic method, called AES. AES is a symmetric key algorithm, which means that the same key is used to encrypt and decrypt. The image data is broken down into fixed-size blocks, typically 128 bits, and each block undergoes a number of rounds of substitution, permutation and mixing. The algorithm can be either 128, 192 or 256 bit and thus the security level can be adjusted depending on the sensitivity of the image. In the encryption process, the pixel values are converted into an encrypted binary format that makes the visual content illegible and resistant to attacks such as statistical analysis or unauthorized reconstruction. AES is reversible and deterministic, and if the proper key is applied, the original image can be reconstructed perfectly. It is efficient and thus can be used for large and real time image processing. It has been proven to secure the visual data with regard to its privacy, integrity and secure access while it is being stored or transmitted.

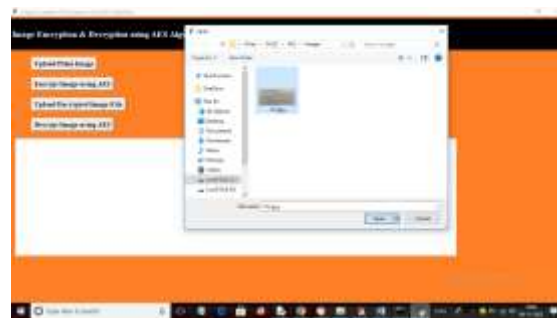
v) AES Encryption: The uploaded images are protected using the Advanced Encryption Standard, a strong and widely-trusted cryptographic technique. AES is a symmetric key algorithm, which means that the same key is used to encrypt and decrypt. The image data is broken down into fixed-size blocks, typically 128 bits, and each block undergoes a number of rounds of substitution, permutation and mixing. The algorithm can be used with key lengths of 128, 192 or 256 bits and so the security level can be adjusted to suit the sensitivity of the image. During encryption, the pixel values are transformed into an encrypted binary format, resulting in a visually meaningless and attack-proof image. These pixel values are encrypted to a form of binary data that can't be used to view or read the image, and is hard to attack by statistical analysis or unauthorized reconstruction. AES is deterministic and reversible – once the proper key is used, the original image can be recovered perfectly. The efficiency of the algorithm makes it suitable for real time and large scale image processing while it's proven cryptographic strength ensures confidentiality, integrity and secure accessibility of digital visual data throughout storage and transmission.

4. Results And Discussions

Click twice on 'run.bat' file, to get the below screen to run project.



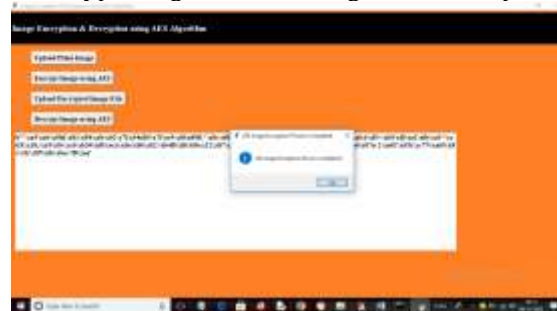
Click on 'Upload Plain Image' button and upload an image to get below output.



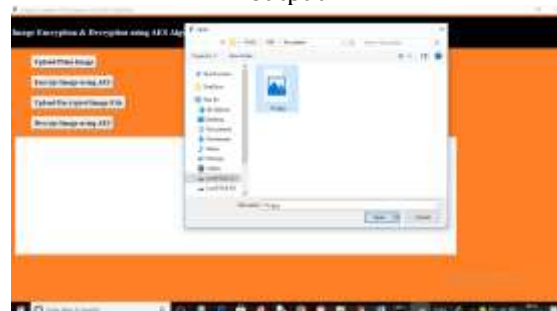
Here we are selecting and uploading images and you can upload any of your image and select that image, then click on 'Open' button to get below output.



In above image is uploaded and when we click on 'Encrypt Image Using AES' button then we will get encrypt image and then we get below output.



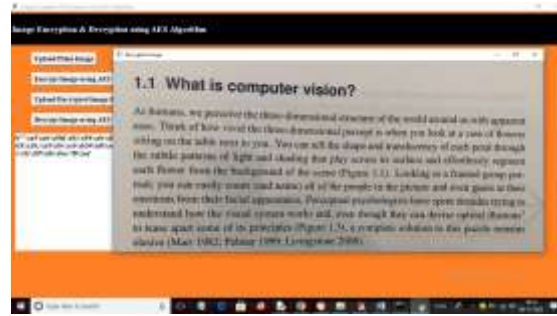
Now in the above screen image, we completed the encryption process and now click on 'OK' button and then click on 'Upload Encrypted Image File' button to re upload the encrypted image and get below output.



Select & upload encrypted image in above screen and then click on 'Open' button to load image and get below output



In the above screen we can see binary encrypted image data loaded and now click on 'Decrypt Image using AES' button to decrypt the above encrypted data and get the below decrypted image



In above screen we have decrypted image from the given encrypted data. You can upload any image and encrypt and decrypt the image as well.

5. Conclusion

The implemented image encryption and decryption method prove that encryption security mechanism implemented as AES is capable of implementing strong cryptographic security in the digital images. The results achieved indicate that the image pixel information can be safely converted into binary encrypted content that is completely unreadable to unauthorized users and thus cannot be accessed or read visually. Successful retrieval of the original image after decryption without any degradation in image quality is a proof of correctness, reversibility and reliability of the encryption process. It can process various image inputs effectively and maintains data integrity throughout the encryption, storage, and decryption process. The work is carried out with high level of confidentiality and resistance of the files to unauthorized analysis: files generated by the work are encrypted and cannot be opened or viewed with common image viewers. The result proves that the self-written AES implementation not only does it give a clearer view of an AES operation, but also achieves the same security level as the industry standard. The results overall will show that the symmetric key cryptography is suitable for protecting multimedia data in real world environment. The proposed work provides a practical framework for the safe storage and transmission of images and the demonstrated approach can be extended to secure video data as well as medical imaging, military surveillance and cloud-based multimedia systems in which data protection and controlled access is vital. Possible enhancements in the future to the encryption framework could be: supporting high resolution multimedia data, supporting real-time video streams, while sustaining performance. DKM, like user-defined keys and key rotation schemes, may add an extra layer of security. The system can be enhanced using AES and asymmetric encryption by providing access control for multiple users and secure key exchange. For large image datasets, optimizations of the performance of the encryption/decryption can be achieved when using parallel processing or GPU acceleration. To enhance the results of robustness evaluation, additional security analysis can be performed, such as resistance to statistical attacks and differential attacks. The framework can be extended to be suitable for cloud and IoT, so that images can be stored and transmitted securely in distributed and resource-limited systems.

References

- [1] Alahe, M. A., Chang, Y., Kemesi, J., Won, K., Yang, X., & Wei, L. (2025). Real-Time agricultural image encryption algorithm using AES on edge computing devices. *Computers and Electronics in Agriculture*, 237, 110594.
- [2] Murugan, M. S., Kumar, U., & TG, S. M. U. (2025, January). Image Encryption for Ensuring Confidentiality and Security Using AES Algorithm. In *2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (pp. 206-212). IEEE.
- [3] Vyshali, S., Yasmeen, W., Swathi, T., & Parvathi, A. (2025, March). Picture Encoding and Decoding Using AES Algorithm. In *International Conference on Advanced Materials, Manufacturing and Sustainable Development (ICAMMSD 2024)* (pp. 753-758). Atlantis Press.
- [4] Banoori, S. Z., Khan, W., Rahman, S., Masood, F., Salam, A., Amin, F., ... & Choi, G. S. (2025). An improved hybrid image steganography method using AES algorithm. *Scientific Reports*.
- [5] Santhosh, B., & Kushmitha, V. (2025, February). Cryptographic Image Security Using AES-XOR Approach. In *2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 13-19). IEEE.
- [6] Dinu, A., & Frunzete, M. (2025). Image encryption using chaotic maps: development, application, and analysis. *Mathematics*, 13(16), 2588.
- [7] Sikder, M. I. H., Sarker, P., Hasan, M. T., & Kadir, M. I. (2025, February). Reusable Block AES: A Modified AES Algorithm for the Encryption and Decryption of Sensitive Data. In *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)* (pp. 1-6). IEEE.

- [8] Pawar, S., Doshi, N., Dhumal, S., & Gaikwad, G. (2025, March). Encryption and Decryption of Different File Format Using AES. In 2025 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-5). IEEE.
- [9] Yogi, B., Khan, A. K., & Roy, S. (2025). Cellular automata based key distribution for lightweight hybrid image encryption with elliptic curve cryptography. *Scientific Reports*, 15(1), 34437.
- [10] Boobalan, S., & Gurunathan Arthanari, S. K. (2025). Lorenz and Chua Chaotic Key-Based Dynamic Substitution Box for Efficient Image Encryption. *Symmetry*, 17(8), 1296.
- [11] El-Rahman, S. A., Mansour, A. E., Jamel, L., Alohal, M. A., Seifeldin, M., & Alkady, Y. (2025). C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC. *IEEE Access*, 13, 41367-41381.
- [12] Gondowarsito, W. (2025). Multi-Format Data Encryption and Decryption with AES Cipher Block Chaining in Python. *Crossroad Research Journal*, 2(2), 56-65.
- [13] Liu, Y., Hu, H., Gao, Y., Hu, S., Yu, Q., Chen, T., & Liu, Y. (2025). An Image Encryption Algorithm Based on HNN with Memristor. *International Journal of Bifurcation and Chaos*, 35(04), 2550043.
- [14] Husam, S., Hoomod, H. K., & Hussein, K. A. (2025). Hybrid Algorithm (DES-Present) for encryption image color using 2D-Chaotic System. *Mustansiriyah Journal of Pure and Applied Sciences*, 3(1), 49-63.
- [15] Sihwail, R., & Ibrahim, D. (2025). A New Image Encryption Method Using an Optimized Smart Codebook. *Human Behavior and Emerging Technologies*, 2025(1), 7807003.
- [16] Wandile, P. S., Kirar, B. S., Jain, S., & Sahu, Y. (2025, January). Compact and Secure Image Encryption for IoT Systems Employing ECC and AES Hybrid Cryptography. In 2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (pp. 1-6). IEEE.
- [17] Ulutas, H. (2025). A novel memristor-based hyperchaotic hybrid encryption system with DNA for image encryption on the Jetson TX2. *Scientific Reports*, 15(1), 35745.
- [18] Saini, A., & Sehrawat, R. (2025). An intelligent and efficient CNN-AES framework for image block encryption with a multi-key approach. *Engineering Research Express*, 7(1), 015206.
- [19] Vayadande, K. (2025). Image encryption decryption using hybrid cryptography. In *Intelligent Data-Driven Techniques for Security of Digital Assets* (pp. 29-48). CRC Press.
- [20] Maiti, P., Paul, M. A. K., & Acharya, M. (2025, February). Comparative Study of Asymmetric Key Cryptographic Algorithms in Image Encryption. In 2025 International Conference on Computer, Electrical & Communication Engineering (ICCECE) (pp. 1-5). IEEE.
- [21] Selvi, J. H. A., & Rajendran, T. (2025). DNA Encoding and Chaos based Image Encryption Technique for Cloud Storage and Communications. *Indian Journal of Science and Technology*, 18(9), 734-744.
- [22] Balayogi, G., & Lakshmi, A. V. (2025). Image encryption via second-order derivative structures: a Hessian-based approach. *International Journal of Information Technology*, 17(8), 4707-4718.
- [23] Alsaraireh, S., Ahmad, A., & AbuHour, Y. (2025). New Step in Lightweight Medical Image Encryption and Authenticity. *Mathematics*, 13(11), 1799.
- [24] Gu, M., Xu, S., Wu, H., & Zhang, P. (2025, July). Lightweight Image Encryption Algorithm Based on Round-Reduced SM4. In 2025 10th International Conference on Signal and Image Processing (ICSIP) (pp. 01-08). IEEE.
- [25] Zou, W., Xin, R., Han, C., & Gao, L. (2025). Research on Image Recognition Technology in the Encryption and Decryption Process of Electronic Archives Driven by Computer Vision. *International Journal of High Speed Electronics and Systems*, 2540379.