Adaptive Encryption and Intelligent Steganography for Secure Data Protection

ASMA KARIM[1], Dr.CH. BUCHI REDDY[2]
[1]Student, Department of Computer Science and Engineering, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Assistant Professor & HOD, Department of Data Science, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Email: buchireddy2017@gmail.com

***Abstract*— The rapid growth of digital technologies has led to an enormous increase in the amount of sensitive information shared and stored across online platforms. As organizations increasingly rely on cloud services, peer-to-peer networks, and blockchain-based systems, ensuring the privacy and security of user data has become a critical concern. Although encryption techniques are widely used to safeguard information, data stored on external servers remains vulnerable to unauthorized access, particularly from insider threats. To overcome this issue, this study presents a secure data protection framework that combines adaptive hybrid encryption with intelligent steganography to provide multiple layers of security. The proposed approach integrates AES and ECC algorithms, allowing secure key management while preventing any single entity from accessing the complete decryption process. In addition, encrypted data is embedded within digital images using image steganography, making the existence of confidential information difficult to detect. Image-based techniques are selected because they offer an effective balance between security and computational efficiency. A hash value is generated for every uploaded file to verify data integrity, while multi-factor authentication using an email-based one-time password strengthens user verification. The system also includes cybersecurity awareness resources and security updates, providing users with a secure, reliable, and user-friendly platform for protecting confidential digital information.**

***Keywords*— Cybersecurity, Hybrid Encryption, Adaptive Encryption, Image Steganography, Data Protection, AES, Elliptic Curve Cryptography (ECC), Multi-Factor Authentication.**

I. INTRODUCTION

The rapid growth of digital communication and cloud-based technologies has increased the amount of sensitive information shared through online platforms. As businesses and individuals rely heavily on digital systems, protecting confidential data from cyber threats has become a major concern. Traditional encryption techniques provide a basic level of security, but the increasing sophistication of cyberattacks requires stronger and multi-layered protection mechanisms. Combining cryptography with data hiding techniques has emerged as an effective solution for improving confidentiality and preventing unauthorized access. Image steganography further enhances security by concealing encrypted information within digital images, making the existence of sensitive data difficult to detect. Allwadhi et al. proposed an image steganography technique based on LSB and Shannon–Fano encoding to improve secure communication [1]. Mahmood and Tabassum introduced a hybrid cryptographic model for secure data protection and efficient key management [2]. Madavi and Karthick demonstrated that integrating cryptography with steganography significantly strengthens cloud data security [7].

Traditional cryptographic algorithms are widely used to protect digital information, but they often face challenges related to key management, computational overhead, and scalability. Symmetric encryption algorithms provide fast data processing, while asymmetric algorithms offer secure key exchange and authentication. The Advanced Encryption Standard (AES) is recognized for its speed and reliability in encrypting large volumes of data. In contrast, Elliptic Curve Cryptography (ECC) provides strong security using smaller key sizes, making it suitable for resource-constrained devices such as IoT sensors and mobile systems. Combining AES and ECC creates a hybrid encryption framework that improves both security and efficiency. Badhan et al. demonstrated the effectiveness of AES in protecting IoT-based smart farming data [3]. Their later work highlighted the importance of end-to-end encryption for secure cloud environments [4]. G et al. integrated ECC with LSB steganography to enhance data security while

maintaining computational efficiency in IoT applications [8].

Hybrid encryption combines the strengths of symmetric and asymmetric cryptographic techniques to provide secure and efficient communication. In this approach, AES is used to encrypt user data quickly, while ECC protects the encryption keys through secure key exchange. This combination improves confidentiality and reduces the risk of unauthorized key access without increasing computational complexity. Hybrid encryption is particularly suitable for cloud computing, mobile applications, and IoT systems where both performance and security are essential. Sahoo et al. proposed a hybrid encryption algorithm that secures sensitive information before hiding it using steganography [13]. Hapsari et al. combined RSA cryptography with an End of File steganography technique to improve data protection [12]. Yahia and Abushaala integrated cryptography with edge detection and LSB steganography to strengthen secure data hiding [6].

Although encryption protects the content of digital information, it does not hide the presence of encrypted files from attackers. Steganography addresses this limitation by embedding encrypted information inside digital images, making confidential data difficult to identify. Image-based steganography is widely preferred because it offers better computational efficiency than audio or video-based techniques while maintaining high security. Integrating encryption with steganography creates multiple layers of protection against unauthorized access. Kumar et al. combined AES encryption with LSB steganography to improve the security of image and text data [9]. Krishna et al. presented a secure data concealment method using RSA cryptography and steganography [5]. Negi and Negi demonstrated the effectiveness of combining AES and LSB techniques for secure image-based data hiding [15].

Modern cybersecurity requires a comprehensive security framework that protects data confidentiality, integrity, and user authentication. In addition to encryption and steganography, mechanisms such as hash-based integrity verification and multi-factor authentication improve overall system security by preventing unauthorized modifications and access. A unified security framework can provide reliable protection while maintaining system performance and usability. Shidaganti et al. proposed a cloud security framework that combines cryptography with image steganography to secure stored information [10]. Chinnasamy et al. enhanced IoT security by integrating elliptic cryptography with advanced steganography techniques [11]. Arora et al. developed a hybrid image security model using steganography and asymmetric cryptography for stronger data protection [14]. Motivated by these studies, this work proposes a secure framework that combines adaptive encryption and intelligent steganography to protect confidential digital information.

II. RELATED WORK

Allwadhi et al., (2023) [1] proposed a hybrid image steganography technique that combines the Least Significant Bit (LSB) method with Shannon–Fano encoding to improve the security of hidden information. Their approach first compresses the secret message using Shannon–Fano encoding before embedding it into a digital image through the LSB technique. This combination helps increase the amount of data that can be concealed while reducing the possibility of detection. The authors evaluated the proposed method using image quality metrics and demonstrated that the visual quality of the cover image remains nearly unchanged after embedding the secret data. The study also highlighted that combining compression with steganography enhances storage efficiency and transmission security. Experimental results showed that the proposed technique provides reliable data hiding with low computational complexity. This work demonstrates that integrating encoding techniques with image steganography can improve both security and embedding efficiency for secure digital communication.

Mahmood and Tabassum, (2021) [2] introduced a hybrid cryptographic data security system that utilizes a Fuzzy Vault key mechanism to strengthen data protection. Their research focused on improving the confidentiality of sensitive information by integrating multiple cryptographic methods with secure key management. The proposed framework generates protected encryption keys that are resistant to unauthorized access while maintaining efficient encryption and decryption operations. The authors discussed how the hybrid approach minimizes the risks associated with key exposure and enhances overall system reliability. Performance analysis showed that the model provides better protection compared to conventional single-algorithm encryption techniques. The study also emphasized that secure key generation is equally important as the encryption process itself. The proposed method offers an effective solution for protecting confidential information in modern communication systems. This research contributes to the development of reliable hybrid cryptographic frameworks for secure digital data storage and transmission.

Badhan et al., (2024) [3] presented an AES-based cryptographic framework to secure smart farming data generated by Internet of Things devices. The study addressed the growing need to protect agricultural information collected from connected sensors and smart monitoring systems. The authors implemented the Advanced Encryption Standard to ensure that transmitted data remains confidential throughout the communication process. Their work demonstrated that AES provides fast encryption with strong resistance against common security attacks while maintaining efficient system performance. The proposed framework was developed within an agile software development environment, enabling flexible implementation and continuous improvement. Experimental evaluation indicated that the encryption mechanism effectively protects farming data without introducing significant computational overhead. The authors concluded that AES is a practical and reliable solution for securing IoT-based agricultural applications. Their research highlights the importance of adopting lightweight yet robust cryptographic techniques for protecting sensitive information in smart farming environments.

Kumar et al., (2022) [9] proposed a hybrid security model that combines AES cryptography with Least Significant Bit steganography to improve the protection of image and text data. In the proposed approach, sensitive information is first encrypted using the AES algorithm before being embedded into a digital image through the LSB technique. This dual-layer security mechanism ensures that even if the hidden data is discovered, it remains protected by encryption. The authors evaluated the effectiveness of their method using image quality measurements and security analysis. Their findings showed that the hybrid model preserves the visual appearance of the cover image while maintaining strong confidentiality of the embedded information. The study also demonstrated that the proposed approach offers higher security than using encryption or steganography individually. This research confirms that integrating cryptographic algorithms with image-based data hiding techniques provides a practical solution for secure digital communication.

Shidaganti et al., (2024) [10] developed a secure cloud data protection framework by integrating cryptographic techniques with image steganography. Their research focused on protecting confidential information stored in cloud environments from unauthorized access and potential cyber threats. The proposed system encrypts sensitive data before embedding it into digital images, creating multiple layers of security for cloud storage. The authors emphasized that combining encryption with steganography significantly improves confidentiality because the existence of secret information remains concealed from attackers. Performance evaluation demonstrated that the framework provides reliable data protection while maintaining acceptable computational efficiency for cloud applications. The study also discussed the advantages of adopting layered security mechanisms to strengthen privacy in distributed computing environments. The authors concluded that integrating cryptography and image steganography offers an effective solution for enhancing cloud security. Their work provides valuable guidance for designing secure and scalable cloud-based data protection systems.

III. DATASET DETAILS

The dataset used in this project consists of user files and text messages that are processed through a secure hybrid encryption and steganography framework for protecting sensitive digital information. Instead of using a publicly available dataset, the system works with user-generated data such as text documents, PDF files, images, and other digital files uploaded through the application. During processing, each uploaded file is encrypted using a combination of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC), ensuring secure data confidentiality and key management. The encrypted information can also be concealed within digital images using image steganography, providing an additional layer of protection. Along with the encrypted file, the system stores important details including the username, file name, upload date, security type, and a unique SHA-256 hash value for integrity verification. This structured dataset enables secure storage, retrieval, and verification of confidential information while supporting different file types and maintaining high levels of privacy throughout the data protection process.

Before storing the uploaded information, several preprocessing and security operations are performed to improve reliability and maintain data integrity. The system validates user credentials through email-based One-Time Password (OTP) authentication before allowing secure file uploads. Each file is encrypted using the hybrid AES-ECC encryption mechanism, after which a SHA-256 hash value is generated to detect any unauthorized modifications. When users choose the steganography option, the encrypted message is converted into binary format and embedded within a selected image using the Least Significant Bit (LSB) technique. The processed files, encrypted content, generated hash codes, upload dates, and security methods are then stored in the database for future retrieval. During data access, the stored hash value is used to verify

file integrity, while the decryption and message extraction processes recover the original information securely. These preprocessing and validation steps ensure that the dataset remains accurate, protected, and suitable for secure storage and communication.

IV. PROPOSED METHODOLOGY

The proposed system adopts a multi-layered security approach to protect sensitive digital information using hybrid encryption and image steganography. Initially, a registered user logs into the application through a secure authentication process that includes email-based One-Time Password (OTP) verification. After successful authentication, users can upload files that need to be protected. The uploaded files are processed using a hybrid encryption mechanism that combines the Advanced Encryption Standard (AES) for fast data encryption and Elliptic Curve Cryptography (ECC) for secure key management. Once the encryption process is completed, a unique SHA-256 hash value is generated for each file to maintain data integrity and detect unauthorized modifications. The encrypted files are securely stored on the server along with their metadata, including filename, upload date, security type, and hash value. For confidential message transmission, users can also embed encrypted text inside digital images using the Least Significant Bit (LSB) image steganography technique, providing an additional layer of protection.

After the data is securely stored, users can access their protected files through the Access Data module. During retrieval, the system verifies the stored hash value to ensure that the file has not been altered. Hybrid encrypted files are decrypted using the corresponding AES and ECC keys before being downloaded by authorized users. For steganographic images, the hidden message is extracted and displayed without affecting the visual quality of the image. In addition to data protection features, the application includes Learning Tools and News Updates modules to improve users' awareness of current cybersecurity practices and emerging threats. The overall framework combines secure authentication, hybrid encryption, steganography, integrity verification, and user education to provide a reliable, efficient, and user-friendly solution for protecting confidential digital information against unauthorized access and cyber threats.

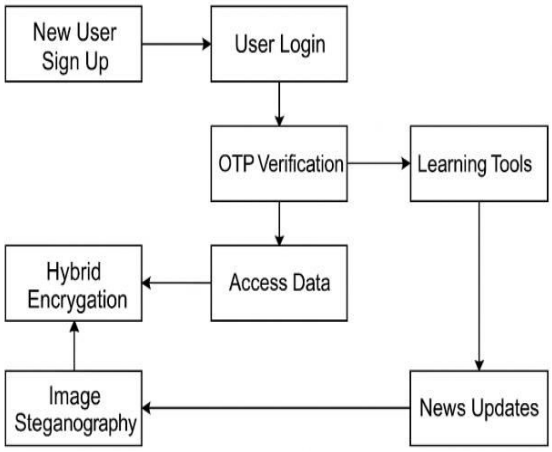

Figure 1: Proposed Data Protection Framework

Figure 1 shows the workflow of the proposed secure data protection system. The process starts with New User Sign Up, followed by User Login and OTP Verification for user authentication. After successful verification, users can securely access the system to encrypt files using Hybrid Encryption or hide confidential messages through Image Steganography. The Access Data module allows authorized users to retrieve protected files and hidden information. In addition, the system provides Learning Tools and News Updates to improve cybersecurity awareness and keep users informed about the latest security practices.

V. RESULT AND DISCUSSION

The proposed cybersecurity framework was successfully implemented and evaluated by testing all functional modules under different usage scenarios. The system allowed users to register, log in securely through email-based OTP verification, and upload confidential files without any processing issues. Uploaded files were protected using the hybrid encryption mechanism that combines AES for fast data encryption and ECC for secure key management. Secret messages were also successfully embedded into digital images using the Least Significant Bit (LSB) steganography technique without causing noticeable changes to image quality. During data retrieval, the stored SHA-256 hash value was verified to ensure that files remained unchanged and free from unauthorized modifications. Authorized users were able to download encrypted files in their original form after successful decryption and extract hidden messages accurately from steganographic images. The Learning Tools and News Updates modules also functioned correctly by providing useful cybersecurity resources. Overall, the system demonstrated reliable performance, secure data

protection, and efficient execution across all implemented modules.

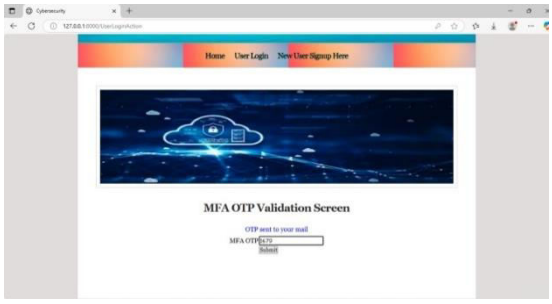

Figure 2: MFA OTP Verification

Figure 2 shows the OTP verification process used for secure user authentication. After login, an OTP is sent to the user's registered email. The user enters the OTP, and upon successful verification, access to the system is granted. This process provides an additional layer of security and prevents unauthorized access.

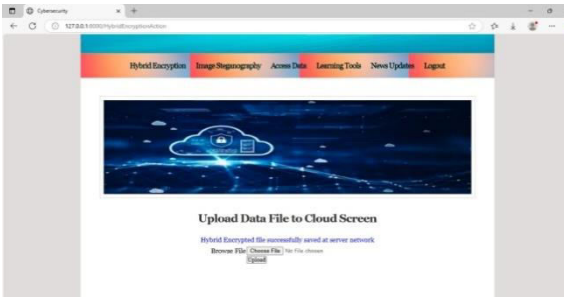

Figure 3: Hybrid Encryption File Upload

Figure 3 shows the Hybrid Encryption module after a file has been uploaded successfully. The selected file is encrypted using the hybrid AES and ECC encryption mechanism before being stored on the server. This process ensures that the uploaded data remains secure and protected from unauthorized access.

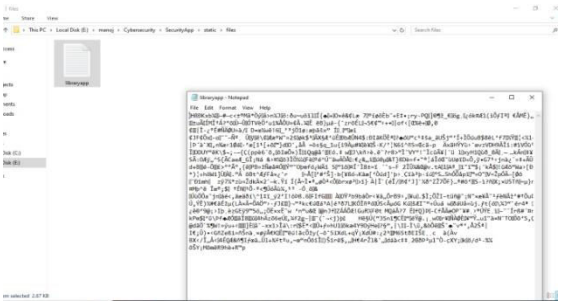

Figure 4: Encrypted File Content

Figure 4 shows the uploaded file after hybrid encryption. The file content appears in an unreadable encrypted format, ensuring that the original information cannot be understood without proper decryption. This confirms that the encryption process has successfully protected the file from unauthorized access.

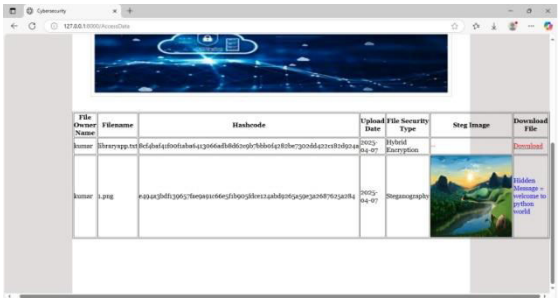

Figure 5: Access Data Module

Figure 5 shows the Access Data module displaying all uploaded files along with their hash values, upload dates, and security types. For steganography files, the system displays the uploaded image and extracts the hidden message. For files protected using Hybrid Encryption, users can click the Download option to retrieve the original file after successful decryption.

Figure 6: Decrypted File Download

Figure 6 shows the downloaded file after successful decryption. The original file content is restored and displayed in a readable format, confirming that the Hybrid Encryption process securely protects the data while allowing authorized users to retrieve the original information correctly.

DISCUSSION

The implementation results indicate that combining hybrid encryption with image steganography provides a stronger security framework than relying on a single protection technique. AES enables efficient encryption of large files, while ECC strengthens key management by providing secure public-key encryption with lower computational requirements. The addition of image steganography further improves confidentiality by concealing encrypted information inside ordinary digital images, making the presence of sensitive data difficult to detect. The use of SHA-256 hash

generation helps verify file integrity and ensures that stored data has not been altered during storage or transmission. Email-based OTP authentication adds another layer of protection by allowing only verified users to access confidential information. The educational modules included in the system encourage users to stay informed about current cybersecurity practices and emerging threats. Overall, the proposed framework delivers a secure, efficient, and user-friendly solution for protecting digital information while maintaining data confidentiality, integrity, and authenticated access.

VI. CONCLUSION

The proposed cybersecurity framework demonstrates an effective approach for protecting sensitive digital information by integrating Hybrid Encryption and Image Steganography within a single security architecture. The combination of AES and ECC provides a balance between fast data encryption and secure key management, ensuring that confidential files remain protected from unauthorized access. In addition, image steganography strengthens security by concealing encrypted messages inside digital images, making the existence of sensitive information difficult to detect. The inclusion of SHA-256 hash generation enables reliable data integrity verification, while email-based Multi-Factor Authentication (MFA) ensures that only authenticated users can access protected resources. Experimental testing confirmed that all system modules, including user authentication, file encryption, steganographic message embedding, secure data retrieval, and integrity verification, functioned successfully without affecting usability. The Learning Tools and News Updates modules further improve user awareness by providing valuable cybersecurity knowledge and current security information. Overall, the proposed framework offers a secure, efficient, and user-friendly solution for protecting digital data in cloud and network environments. Future enhancements may include supporting additional steganography techniques, stronger authentication methods, and optimization for large-scale cloud and IoT applications to further improve system performance and security.

REFERENCES

[1] S. Allwadhi, K. Joshi, A. K. Yadav, R. Nandal and R. Jain, "A Hybrid Approach Towards Image Steganography Using LSB and Shannon – Fano Encoding Technique," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 1606-1611, doi: 10.1109/ICAC3N60023.2023.10541678.

[2] M. A. Mahmood and T. Tabassum, "A Hybrid Cryptographic Data Security System Utilizing Fuzzy Vault Key," 2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON), Dhaka, Bangladesh, 2021, pp. 89-93, doi: 10.1109/RAAICON54709.2021.9930051.

[3] A. Badhan, S. S. Malhi, H. Singh, G. Kaur and S. Bharany, "Implementation of AES Cryptography to Smart Farming Data using IoT Under Agile Framework," 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2024, pp. 541-546, doi: 10.1109/ICECA63461.2024.10800999.

[4] A. Badhan, H. Vasudev, D. Kapila and H. Himanshu, "Data Security in Cloud Environment Using Cryptography Technique for End-to-End Encryption", E3S Web of Conferences, vol. 556, pp. 01002, 2024.

[5] C. L. Krishna, P. Anudeep, C. S. N. V. Sai Vijaya Lakshmi, M. V. P. Chandra Sekhara Rao, S. V. Chereddy and B. Rama Krishna, "Concealment of Data using RSA Cryptography and Steganography Techniques," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 778-783, doi: 10.1109/ICEARS56392.2023.10085355.

[6] F. F. M. Yahia and A. M. Abushaala, "Cryptography using Affine Hill Cipher Combining with Hybrid Edge Detection (Canny-LoG) and LSB for Data Hiding," 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 2022, pp. 379-384, doi: 10.1109/MI-STA54861.2022.9837714.

[7] K. P. B. Madavi and P. V. Karthick, "Enhanced Cloud Security using Cryptography and Steganography Techniques," 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), Bengaluru, India, 2021, pp. 90-95, doi: 10.1109/CENTCON52345.2021.9687919.

[8] G. G, C. Ashwin, B. V. P, A. A and A. Hiremath, "Enhanced Data Encryption in IOT using ECC Cryptography and LSB Steganography," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 2021, pp. 173-177, doi: 10.1109/ICDI3C53598.2021.00043.

[9] M. Kumar, A. Soni, A. R. S. Shekhawat and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1453-1457, doi: 10.1109/ICAIS53314.2022.9742942.

[10] G. Shidaganti, M. V. L, 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, 2024, pp. 93- 99, doi: 10.1109/I4C62240.2024.10748507.

[11] P. Chinnasamy, R. Kumar Ayyasamy, K. Anuradha, I. Alam, D. M. Narayanan Nair and A. Kiran, "Enhancing IoT Data Security: Integrating Elliptic Galois Cryptography with Matrix XOR Steganography and Adaptive Firefly Optimization," 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2024, pp. 29-33, doi: 10.1109/I-SMAC61858.2024.10714687.

[12] R. K. Hapsari, W. Widodo, B. D. Meilani, T. Kristanto, S. Nurmuslimah and T. Indriyani, "Hybrid Cryptography and Steganography with Rivest Shamir Adleman and End of File Algorithm," 2023 Sixth International Conference on Vocational Education and Electrical Engineering (ICVEE), Surabaya, Indonesia, 2023, pp. 291-296, doi: 10.1109/ICVEE59738.2023.10348301.

[13] A. K. Sahoo, A. Nawroz and V. K. Mishra, "Hybrid Encryption Algorithm to Encrypt Sensitive Information and Hiding it Using Steganography," 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2023, pp. 1338-1341, doi: 10.1109/ICAC3N60023.2023.10541624.

[14] H. Arora, R. Agarwal, P. Sharma, G. Shankar and D. Arora, "Image Security Utilizing Hybrid Model of Steganography and Asymmetric Cryptography Methods," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 277-280, doi: 10.1109/IDCIoT56793.2023.10053432.

[15] L. Negi and L. Negi, "Image Steganography Using Steg with AES and LSB," 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2021, pp. 1- 6, doi: 10.1109/ICCED53389.2021.9664834.