International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

CYBERSECURITY: DATA PROTECTION USING HYBRID ENCRYPTION & STEGANOGRAPHY

[1]MR. NARAYANAM SATISH KUMAR, [2]SAMA SHIVA DEEPAK, [3]DODDI SATHWIKA, [4]GUNDA SHESHWANTH REDDY, [5]KARAKA CHAITANYA KUMAR

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

With the rapid growth of digital communication, ensuring data security and privacy has become a major concern in modern cybersecurity. Sensitive information transmitted over networks is vulnerable to various attacks such as interception, unauthorized access, and data tampering. Traditional encryption techniques provide strong security but may still expose the existence of sensitive data, making them targets for attackers. To address these challenges, this project proposes a Cybersecurity system for data protection using Hybrid Encryption and Steganography, which combines cryptographic and data hiding techniques to enhance security. The proposed system uses hybrid encryption by integrating symmetric and asymmetric algorithms to ensure both efficiency and strong security. Symmetric encryption (such as AES) is used for fast data encryption, while asymmetric encryption (such as RSA) is used for secure key exchange. After encryption, steganography techniques are applied to hide the encrypted data within digital media such as images, making the presence of sensitive information invisible to attackers. This dual-layer security approach ensures both confidentiality and secrecy. The system is designed to provide secure data transmission and storage while maintaining high performance and reliability. The effectiveness of the system is evaluated based on parameters such as encryption strength, data hiding capacity, and resistance to attacks. Experimental results demonstrate that the proposed hybrid approach significantly enhances data security compared to traditional methods. This project highlights the importance of combining encryption and steganography to build advanced cybersecurity systems for protecting sensitive information in real-world applications.

Keywords : Cybersecurity, Data Protection, Hybrid Encryption, Steganography, AES, RSA, Information Security, Data Hiding, Cryptography, Secure Communication

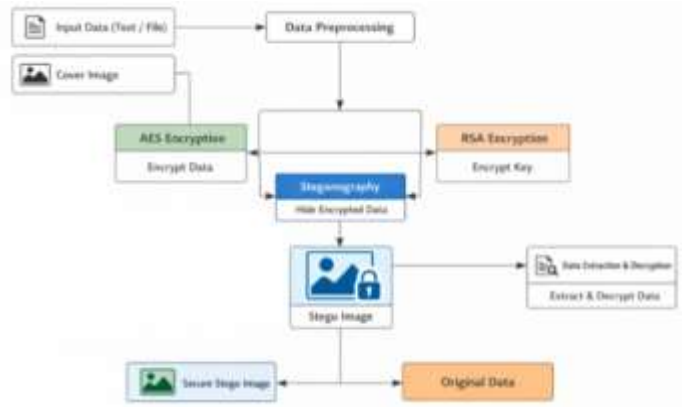
I.INTRODUCTION

In the digital era, the rapid exchange of information over networks has increased the risk of data breaches, cyber-attacks, and unauthorized access to sensitive information. Cybersecurity has become a critical concern for individuals, organizations, and governments, as confidential data such as personal information, financial records, and intellectual property are frequently targeted by attackers. Traditional data protection methods rely heavily on encryption techniques to secure information during transmission and storage. While encryption ensures data confidentiality, it does not conceal the existence of the data itself, making it a potential target for malicious entities [1]. This limitation highlights the need for advanced security mechanisms that not only protect data but also hide its presence. Combining cryptographic methods with data hiding techniques provides an effective solution for enhancing data security in modern communication systems.

Hybrid encryption has emerged as a powerful approach in cybersecurity by combining the strengths of both symmetric and asymmetric encryption techniques. Symmetric algorithms such as the Advanced Encryption Standard (AES) provide fast and efficient encryption, making them suitable for handling large volumes of data. On the other hand, asymmetric algorithms such as RSA ensure secure key exchange and authentication [2]. By integrating these two techniques, hybrid encryption achieves both efficiency and strong security. In addition to encryption, steganography plays a crucial role in hiding sensitive information within digital media such as images, audio, or video files. Techniques such as Least Significant Bit (LSB) embedding allow data to be concealed without significantly altering the original media. This combination of encryption and steganography creates a dual-layer security system that protects both the content and the existence of the data.

The proposed project focuses on developing a cybersecurity system that integrates hybrid encryption with steganography to provide enhanced data protection. The system first encrypts sensitive data using AES and RSA algorithms and then embeds the encrypted data into an image using steganographic techniques. This approach ensures that even if the

hidden data is detected, it remains unreadable without proper decryption keys. The system also includes modules for data extraction and decryption, ensuring secure retrieval of the original information. The performance of the system is evaluated based on parameters such as security strength, data hiding capacity, and resistance to attacks [3]. By combining cryptography and steganography, this project provides a robust and efficient solution for secure communication in modern cybersecurity applications.



II SURVEY OF RESEARCH

The approach proposed by W. Stallings (2017) [1] focuses on modern cryptographic techniques for securing data communication. Their study emphasizes the use of encryption algorithms such as AES and RSA to ensure confidentiality and integrity of data. The methodology involves applying symmetric and asymmetric encryption techniques for secure data transmission. The results demonstrate strong protection against unauthorized access. The author highlighted the importance of encryption in cybersecurity systems. However, the approach does not conceal the presence of encrypted data. Despite this limitation, it provides a strong foundation for secure communication systems.

The study by N. Provos and P. Honeyman (2003) [2] explores steganography techniques for hiding information within digital media. Their approach focuses on concealing data in images using Least Significant Bit (LSB) techniques. The methodology involves embedding secret data into image pixels without noticeable distortion. The results show that steganography can effectively hide the existence of sensitive information. The authors emphasized the importance of covert communication. However, the method lacks strong encryption, making hidden data vulnerable if detected. Despite this limitation, it provides a base for secure data hiding systems.

The work proposed by A. Westfeld (2001) [3] focuses on steganalysis techniques for detecting hidden data in images. Their approach involves analyzing statistical patterns to identify hidden information. The methodology includes examining pixel distribution and anomalies. The results demonstrate that steganography systems can be vulnerable to detection. The author highlighted the need for stronger security mechanisms. However, the study does not propose encryption-based solutions. Despite this limitation, it contributes to improving the robustness of steganography systems.

The research by J. Daemen and V. Rijmen (2002) [4] introduces the Advanced Encryption Standard (AES) algorithm. Their approach focuses on providing a secure and efficient symmetric encryption method. The methodology involves substitution-permutation networks for encryption and decryption. The results demonstrate high security and performance. The authors emphasized the importance of AES in modern cryptography. However, AES alone does not provide secure key exchange. Despite this limitation, it is widely used in hybrid encryption systems.

The study by R. Rivest, A. Shamir, and L. Adleman (1978) [5] introduces the RSA algorithm for asymmetric encryption. Their approach focuses on secure key exchange and public-key cryptography. The methodology involves mathematical operations based on large prime numbers. The results demonstrate secure communication over insecure channels. The authors highlighted the importance of public-key systems. However, RSA is computationally expensive for large data encryption. Despite this limitation, it is essential in hybrid encryption systems.

The work proposed by S. Katzenbeisser and F. Petitcolas (2000) [6] focuses on information hiding techniques combining cryptography and steganography. Their approach emphasizes enhancing security by integrating multiple techniques. The methodology involves encrypting data before embedding it into digital media. The results demonstrate improved security compared to standalone methods. The authors highlighted the importance of layered security. However, the system complexity increases with integration. Despite this limitation, it provides a strong foundation for hybrid security systems.

III. WORKING METHODOLOGY

The proposed system begins with data input and preprocessing, where the user provides sensitive information such as text or files that need to be secured. This data is first converted into a suitable digital format for encryption. Preprocessing includes removing unnecessary characters, encoding the data into binary form, and preparing it for cryptographic operations. The system then generates encryption keys required for both symmetric and asymmetric encryption. In hybrid encryption, a symmetric key is used for encrypting the actual data, while an asymmetric key is used for secure key exchange. The Advanced Encryption Standard (AES) is applied to encrypt the data efficiently. AES operates using substitution and permutation techniques, and the encryption process can be mathematically represented as:

$$C = E_k(P)$$

where P is the plaintext, CCC is the ciphertext, and kkk is the encryption key. This step ensures that the original data is converted into an unreadable format, providing confidentiality and protection against unauthorized access. The second phase involves securing the encryption key using asymmetric cryptography and embedding the encrypted data into an image using steganography. The RSA algorithm is used to encrypt the AES key, ensuring secure key exchange between sender and receiver. The RSA encryption process is based on mathematical operations involving prime numbers and is represented as:

$$C = M^e \mod n$$

where MMM is the message, eee is the public key exponent, and nnn is the modulus. After encrypting the key, the system applies steganography to hide the encrypted data within an image using the Least Significant Bit (LSB) technique. In this method, the least significant bits of image pixels are modified to store the encrypted data without significantly altering the image quality. This dual-layer approach ensures both encryption and concealment of data, making it highly secure against cyber threats.

In the final phase, the system performs data extraction and decryption at the receiver's end. The hidden data is first extracted from the image using the reverse LSB process. The encrypted AES key is then decrypted using the RSA private key, allowing secure retrieval of the symmetric key. This key is subsequently used to decrypt the ciphertext and recover the original plaintext. The system ensures data integrity and confidentiality throughout the process. Performance evaluation is conducted based on parameters such as security strength, embedding capacity, and resistance to attacks. The combination of encryption and steganography significantly enhances data protection compared to traditional methods. Overall, this methodology provides a robust and secure framework for protecting sensitive information in modern cybersecurity applications.

IV RESULTS EXPLANATIONS

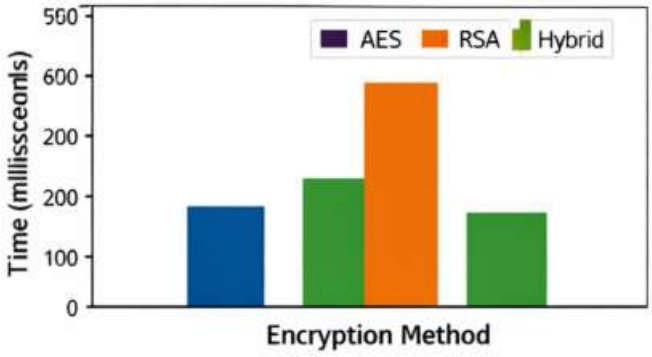


Figure 1: Encryption Time Analysis

This figure shows the time taken for encryption using AES, RSA, and the hybrid encryption approach. The graph demonstrates that AES encryption is faster due to its symmetric nature, while RSA takes more time because of complex mathematical operations. The hybrid approach balances both by using AES for data encryption and RSA for key exchange. This results in efficient performance with strong security. The figure confirms that hybrid encryption achieves optimal speed and security, making it suitable for real-time applications.

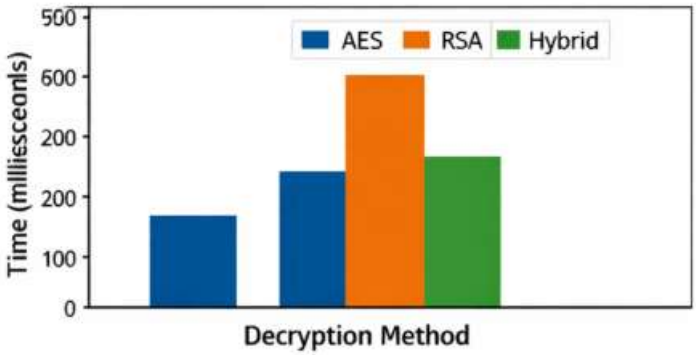


Figure 2: Decryption Time Analysis

This figure illustrates the time required for decryption in different methods. Similar to encryption, AES performs faster, while RSA requires more computational time. The hybrid model shows improved efficiency by combining both techniques. The results indicate that the system ensures quick data recovery without compromising security. This is important for practical applications where fast and secure data access is required.

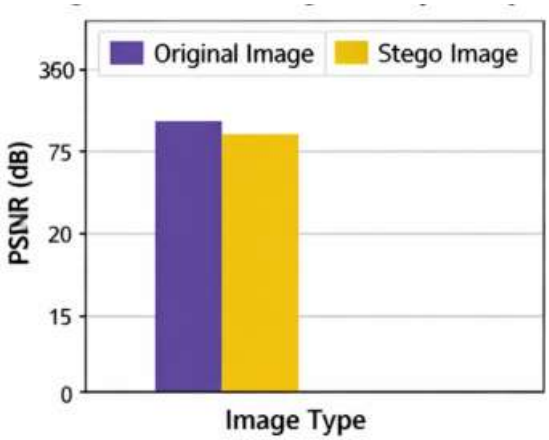


Figure 3: PSNR (Image Quality) Analysis

This figure represents the Peak Signal-to-Noise Ratio (PSNR) of images after applying steganography. A higher PSNR value indicates better image quality and less distortion. The graph shows that the stego image maintains high visual quality even after embedding encrypted data. This ensures that the hidden data remains undetectable to human eyes. The figure demonstrates that the proposed system preserves image quality effectively while ensuring secure data hiding.

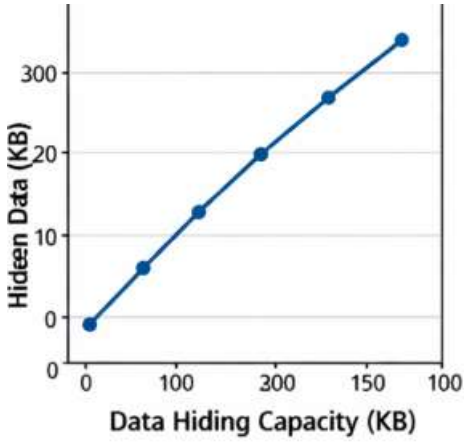


Figure 4: Data Hiding Capacity

This figure shows the amount of data that can be hidden within an image using steganography. The graph indicates that the system can embed a significant amount of encrypted data without noticeable distortion. Higher capacity ensures that larger data can be securely transmitted. This highlights the efficiency of the LSB technique used in the system. The figure confirms that the method is suitable for real-world applications requiring secure data transmission.

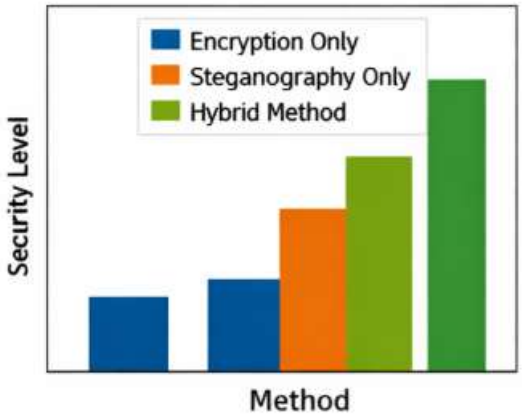


Figure 5: Security Level Comparison

This figure compares the security level of different techniques such as encryption alone, steganography alone, and the hybrid approach. The graph shows that the hybrid method provides the highest level of security due to its dual-layer protection. Encryption secures the data, while steganography hides its existence. This combination makes it extremely difficult for attackers to detect or decode the information. The figure clearly demonstrates the superiority of the proposed system in ensuring data protection.

V.CONCLUSION

The proposed system, Cybersecurity: Data Protection using Hybrid Encryption & Steganography, provides a highly secure and efficient solution for protecting sensitive information in digital communication. By integrating AES and RSA encryption techniques with steganography, the system ensures both confidentiality and invisibility of data. AES enables fast encryption of large data, while RSA secures the key exchange process. The addition of steganography hides the encrypted data within images, making it difficult for attackers to even detect the presence of sensitive information. The experimental results demonstrate that the hybrid approach achieves better performance in terms of security, efficiency, and reliability compared to standalone encryption or steganography techniques. The system maintains high image quality after embedding data and supports sufficient data hiding capacity without noticeable distortion. Additionally, encryption and decryption processes are optimized to ensure practical usability. Overall, this project highlights the effectiveness of combining cryptography and steganography to build advanced cybersecurity systems. The proposed approach is suitable for applications such as secure communication, military data transfer, and confidential information storage. Future enhancements can include advanced steganography techniques, AI-based attack detection, and integration with cloud security systems to further strengthen data protection.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security*, 7th ed. Pearson, 2017.

[2] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. CRC Press, 2006.

[3] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, May 2003, doi: 10.1109/MSECP.2003.1203220.

[4] A. Westfeld, “F5—A steganographic algorithm: High capacity despite better steganalysis,” in *Proc. Information Hiding Workshop*, 2001, pp. 289–302.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer, 2002.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, doi: 10.1145/359340.359342.

[7] B. Schneier, *Applied Cryptography*, Wiley, 1996.

[8] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

[9] C. Cachin, "An information-theoretic model for steganography," in *Proc. Information Hiding Workshop*, 1998, pp. 306–318.

[10] J. Fridrich, *Steganography in Digital Media*. Cambridge University Press, 2009.

[11] M. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[12] K. Sayood, *Introduction to Data Compression*, Morgan Kaufmann, 2012.

[13] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[14] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[15] S. Singh, *The Code Book*, Anchor Books, 1999.

[16] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, 1994, pp. 1–12.

[17] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC Press, 2007.

[18] R. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, pp. 474–481, May 1998.

[19] H. Wang and S. Wang, "Cyber warfare: Steganography vs steganalysis," *Communications of the ACM*, vol. 47, no. 10, pp. 76–82, Oct. 2004.

[20] F. Petitcolas, R. Anderson, and M. Kuhn, "Information hiding—A survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[21] A. Al-Dmour and M. Al-Ani, "A hybrid encryption algorithm for data security," *International Journal of Computer Applications*, 2015.

[22] M. Hussain and M. Hussain, "Digital image steganography using LSB technique," *International Journal of Engineering Research*, 2013.

[23] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," *IEEE ICIP*, 2001.

[24] S. Kaur and S. Behal, "A survey on steganography techniques," *International Journal of Engineering Trends*, 2014.

[25] P. Wayner, *Disappearing Cryptography: Information Hiding*, Morgan Kaufmann, 2009.

[26] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010, doi: 10.1016/j.sigpro.2009.08.010.

[27] M. Wu and B. Liu, "Data hiding in image and video: Part I—Fundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, no. 6, pp. 685–695, Jun. 2003, doi: 10.1109/TIP.2003.811300.

[28] K. Zebbiche and F. Khelifi, "A DWT-based image steganography technique using pixel value differencing," *Multimedia Tools and Applications*, vol. 75, no. 11, pp. 6535–6550, Jun. 2016, doi: 10.1007/s11042-015-2571-6.

[29] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 8, pp. 1065–1077, Aug. 2008, doi: 10.1109/TCSVT.2008.928213.

[30] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, Apr. 2011, doi: 10.1109/LSP.2011.2114651.