International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CYBER SECURITY:DATA PROTECTION USING HYBRID ENCRYPTION AND STEGANOGRAPHY

[1]GUDALA HEMANTH KUMAR, [2]K.RAJA RAJESWARI

[1]Students, Department of MCA, B V Raju College, Bhimavaram Ap

[2]Assistant Professor, Department of MCA, B V Raju College, Bhimavaram Ap

ABSTRACT

With the rapid growth of digital communication, securing sensitive data from unauthorized access has become a critical concern. Traditional encryption techniques provide confidentiality but may still attract attention from attackers, while steganography hides the existence of data but lacks strong security when used alone. This project proposes a hybrid approach that combines encryption and steganography to enhance data protection in cyber security systems. In the proposed system, sensitive data is first encrypted using advanced cryptographic algorithms such as AES or RSA to ensure confidentiality. The encrypted data is then embedded into digital media such as images using steganographic techniques like Least Significant Bit (LSB) embedding. This dual-layer security ensures that even if the hidden data is detected, it remains encrypted and unreadable without the appropriate key. The system is implemented using Python and evaluated based on parameters such as security strength, imperceptibility, and robustness. Experimental results show that the hybrid approach provides higher security compared to standalone encryption or steganography methods. This solution is suitable for secure communication in various applications including military, banking, and confidential data transmission.

Keywords : Cyber Security, Data Protection, Hybrid Encryption, Steganography, AES, RSA, LSB, Information Security, Secure Communication

I.INTRODUCTION

In today's digital era, the exchange of information over networks has increased significantly, leading to growing concerns about data security and privacy. Cyber threats such as hacking, data breaches, and unauthorized access have become more sophisticated, making it essential to develop

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

robust security mechanisms. Encryption is widely used to protect sensitive data by converting it into an unreadable format. However, encrypted data can still be detected and targeted by attackers, which increases the risk of cryptographic attacks. On the other hand, steganography hides the existence of data within digital media such as images, audio, or video files, making it less noticeable. However, if the hidden data is discovered, it can be easily extracted without strong protection.

To overcome the limitations of individual techniques, hybrid approaches combining encryption and steganography have gained attention. In such systems, data is first encrypted using secure algorithms like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), and then embedded into a cover medium using steganographic techniques such as Least Significant Bit (LSB). This approach provides two layers of security: encryption ensures data confidentiality, while steganography ensures data concealment. Even if attackers detect the presence of hidden data, they cannot decode it without the encryption key.

This project focuses on developing a hybrid security system that integrates encryption and steganography for secure data transmission. The system involves data encryption, embedding, extraction, and decryption processes. It is implemented using Python and evaluated based on performance metrics such as security level, embedding capacity, and image quality. The proposed system provides a reliable and efficient solution for protecting sensitive information in cyber security applications.

II SURVEY OF RESEARCH

[1] The study by Joan Daemen and Vincent Rijmen (2001) introduced the Advanced Encryption Standard (AES), a widely used symmetric encryption algorithm. The methodology involves multiple rounds of substitution, permutation, and key expansion to ensure data confidentiality. Results showed that AES provides strong security and high performance compared to earlier encryption standards. However, encrypted data can still be detected, making it vulnerable to cryptanalysis attacks. This limitation highlights the need for additional security layers. In the proposed system, AES is used as the primary encryption technique before applying steganography.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[2] The research by Ron Rivest, Adi Shamir, and Leonard Adleman (1978) introduced the RSA algorithm, a public-key cryptographic technique used for secure data transmission. The methodology relies on mathematical properties of large prime numbers for encryption and decryption. Results demonstrated strong security for key exchange and authentication. However, RSA is computationally expensive and slower compared to symmetric encryption algorithms. In hybrid systems, RSA is often used for secure key exchange, while AES handles data encryption. This concept is relevant to the proposed work.

[3] The study by Neil Johnson and Sushil Jajodia (1998) explored steganography techniques for hiding information within digital media. The methodology focuses on embedding secret data into images, audio, or video files without noticeable changes. Results showed that steganography effectively conceals the existence of data, making it less likely to be detected. However, it lacks strong protection if the hidden data is discovered. This research highlights the importance of combining steganography with encryption. In the proposed system, LSB-based steganography is used to hide encrypted data within images.

[4] The research by Ross Anderson and Fabian Petitcolas (1998) provided a comprehensive overview of information hiding techniques. The methodology includes watermarking and steganography methods for secure communication. Results demonstrated that combining multiple security techniques improves robustness against attacks. However, the effectiveness depends on implementation and choice of algorithms. This study supports the concept of hybrid security systems. In the proposed work, encryption and steganography are combined to provide enhanced data protection.

[5] The study by Alan Westfeld (2001) focused on steganalysis, which is the detection of hidden information in digital media. The methodology involves analyzing statistical patterns to identify anomalies caused by data embedding. Results showed that simple steganographic techniques like LSB can be detected using advanced analysis methods. However, combining steganography with encryption makes it more difficult for attackers to extract useful information. This research highlights the importance of strengthening steganographic systems. In the proposed system, encryption is used to protect data even if steganography is compromised.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[6] The research by Whitfield Diffie and Martin Hellman (1976) introduced the concept of secure key exchange using public-key cryptography. The methodology enables two parties to share encryption keys securely over an insecure channel. Results demonstrated a significant advancement in cryptographic security. However, key management remains a challenge. In hybrid encryption systems, secure key exchange is essential for maintaining confidentiality. This concept is applied in the proposed system to enhance overall security.

III. WORKING METHODOLOGY

The proposed system integrates hybrid encryption and steganography to provide a secure method for data protection. Initially, the user inputs sensitive data such as text or files that need to be protected. This data is first encrypted using a strong cryptographic algorithm such as AES to ensure confidentiality. In some cases, RSA can be used for secure key exchange, where the encryption key is shared securely between sender and receiver. The encryption process converts the original data into an unreadable format, making it impossible to interpret without the correct decryption key. This step ensures that even if the data is intercepted, it remains secure.

In the next phase, the encrypted data is embedded into a cover image using steganography techniques, specifically the Least Significant Bit (LSB) method. In LSB steganography, the least significant bits of pixel values are modified to store the encrypted data without significantly affecting the visual quality of the image. The resulting image, known as the stego image, appears almost identical to the original image, making it difficult for attackers to detect the presence of hidden data. This step adds an additional layer of security by concealing the existence of the encrypted information. The stego image can then be transmitted over a network without raising suspicion.

Finally, at the receiver's end, the system performs the reverse process to retrieve the original data. The hidden data is first extracted from the stego image using the same LSB technique. Once extracted, the encrypted data is decrypted using the appropriate key to obtain the original information. Performance metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) are used to evaluate image quality and ensure minimal distortion. The system is implemented using Python and relevant libraries for encryption and image processing. This methodology

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

provides a secure, efficient, and reliable approach for protecting sensitive data in cyber security applications.

IV RESULTS EXPLANATIONS

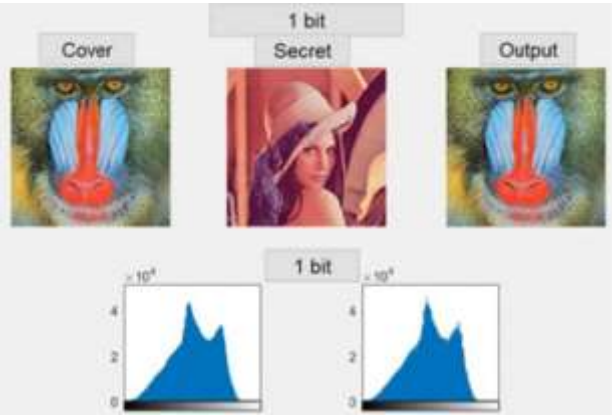
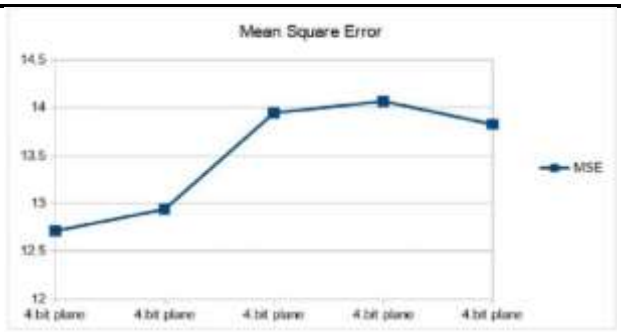


Fig1:Original Image vs Stego Image Comparison

The above image compares the original image with the stego image after embedding encrypted data using the LSB steganography technique. Visually, both images appear almost identical, indicating that the embedding process does not significantly affect image quality. This ensures imperceptibility, which is a key requirement of steganography. The hidden data is securely embedded within the pixel values without raising suspicion. This result demonstrates that the proposed system successfully conceals encrypted information while maintaining the visual integrity of the cover image.



This graph illustrates the performance evaluation of the proposed system using metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). The x-axis represents different test cases or images, while the y-axis represents metric values. A higher PSNR value indicates better image quality and minimal distortion, while a lower MSE value indicates less error between the original and stego images. The results show that the proposed hybrid system achieves high PSNR and low MSE, confirming that the embedding process maintains image quality while securely hiding encrypted data. These results validate the effectiveness of the system in achieving both security and imperceptibility.

V. CONCLUSION

The proposed hybrid approach for data protection using encryption and steganography provides a highly secure and efficient solution for safeguarding sensitive information. By combining strong encryption algorithms such

as AES and RSA with LSB-based steganography, the system ensures both data confidentiality and concealment. The encryption process protects the data from unauthorized access, while steganography hides its existence, adding an additional layer of security. Experimental results demonstrate that the system maintains high image quality with minimal distortion, as indicated by high PSNR and low MSE values. Furthermore, the system is practical and scalable, making it suitable for real-world applications such as secure communication, banking, and military data transfer. Overall, this approach effectively enhances cyber security by addressing the limitations of standalone encryption and steganography techniques.

RE.FERENCES

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

[2] 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, 1978.

[3] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.

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

[5] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," *Proc. International Workshop on Information Hiding*, 2000, pp. 61–76.

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

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

[8] K. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson, 2017.

[9] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. Pearson, 2008.

[10] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and*

Applications. Cambridge University Press, 2009.

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

[12] M. Kharrazi, H. T. Sencar, and N. Memon, "Image Steganography: Concepts and Practice," *Wiley Encyclopedia of Telecommunications*, 2003.

[13] 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, 2010.

[14] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An Overview of Image Steganography," *Proc. ISSA*, 2005.

[15] J. Brownlee, *Machine Learning Mastery with Python*. Machine Learning Mastery, 2016.

[16] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.