INTERNATIONAL JOURNAL OF ECONOMIC SOCIAL SCIENCE AND MANAGEMENT LAW
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3070-0558
VOL.7, NO.2(1) (2026)

CYBERSECURITY: DATA PROTECTION USING HYBRID ENCRYPTION & STEGANOGRAPHY

Alluri Thripura Prasanthi [1], LNV RAO [2]

[1]PG Student, Department of CSE, V.K.R, V.N.B & A.G.K College Of Engineering, Gudivada, AP, India, 521301.
[2]Associate Professor & ACE-1 , Department of CSE, V.K.R, V.N.B & A.G.K College Of Engineering, Gudivada, AP, India, 521301.

E-Mail: prasanthialluri502@gmail.com, lankapalli@gmail.com

ABSTRACT

In the era of rapidly expanding digital communication, ensuring secure data transmission has become a critical concern in cybersecurity. This study proposes a robust data protection framework that integrates hybrid encryption techniques with steganography to enhance confidentiality, integrity, and stealth of sensitive information. The hybrid encryption approach combines the strengths of symmetric encryption for fast data processing and asymmetric encryption for secure key exchange, thereby improving overall security efficiency. To further strengthen protection, steganography is employed to conceal encrypted data within digital media such as images, audio, or video files, making the presence of the secret information undetectable to unauthorized users. This dual-layer security mechanism not only safeguards data from interception and cryptographic attacks but also reduces the risk of detection during transmission. The proposed system is designed to be efficient, scalable, and suitable for real-time applications in areas such as secure communication, military data exchange, and financial transactions.

INTRODUCTION

In today's digital era, the rapid growth of internet usage and online communication has increased the risk of cyber threats such as data breaches, unauthorized access, and information leakage. As sensitive data is frequently transmitted across unsecured networks, ensuring its confidentiality and security has become a major challenge in the field of cybersecurity. Traditional encryption methods provide a certain level of protection, but they may still attract attackers' attention due to the visible presence of encrypted data.

To address these limitations, advanced security techniques such as hybrid encryption and steganography are being widely explored. Hybrid encryption combines symmetric encryption, which is efficient for large data processing, with asymmetric encryption, which ensures secure key exchange between sender and receiver. This combination enhances both performance and security.

In addition, steganography adds another layer of protection by hiding encrypted data within digital media such as images, audio, or video files. This makes the existence of the secret data invisible to unauthorized users, thereby reducing the chances of detection and attack.

By integrating hybrid encryption with steganography, the proposed system aims to provide a highly secure and efficient method for data protection, ensuring safe communication in sensitive applications such as military systems, financial transactions, and confidential data exchange.

LITERATURE SURVEY

1. Title: A Hybrid Cryptographic Approach for Secure Data Transmission
Author: M. Sharma et al.
Description: This study proposes a hybrid encryption model combining AES (Advanced Encryption Standard) and RSA algorithms to improve data security during transmission. The work highlights that symmetric encryption

provides faster processing for large datasets, while asymmetric encryption ensures secure key exchange. The authors conclude that hybrid cryptography significantly enhances both performance and security compared to standalone encryption methods.

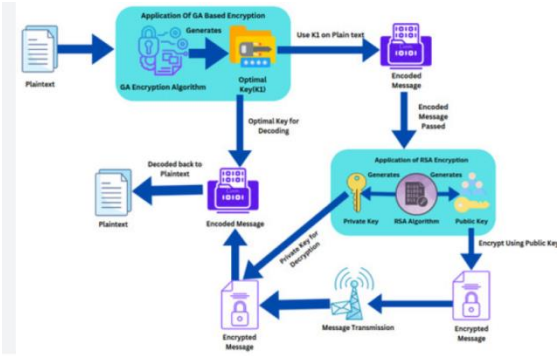
2. Title: Image Steganography for Secure Communication
Author: R. K. Singh and P. Verma
Description: This paper focuses on hiding confidential data within digital images using spatial domain techniques such as Least Significant Bit (LSB) insertion. The study emphasizes that steganography helps in concealing the existence of data, making it less vulnerable to attacks. However, it also notes limitations in terms of robustness against image processing operations.

3. Title: Secure Data Communication Using Combined Encryption and Steganography
Author: A. Gupta et al.
Description: The authors propose a dual-layer security system that integrates encryption techniques with steganography to enhance confidentiality. Encrypted data is first generated and then embedded into multimedia files. The study demonstrates that combining both methods provides higher security compared to using either technique alone.

4. Title: Performance Analysis of Hybrid Encryption Algorithms in Cloud Security
Author: S. Reddy and K. Nair
Description: This research evaluates the efficiency of hybrid encryption methods in cloud environments. It concludes that combining AES with RSA reduces encryption overhead while maintaining strong security. The study also suggests that such hybrid models are suitable for real-time cloud-based applications.

5. Title: Data Hiding Techniques in Steganography: A Survey
Author: J. Thomas and L. Joseph
Description: This survey provides an overview of various steganographic techniques including spatial, transform, and adaptive domain methods. It highlights the importance of selecting appropriate embedding techniques based on security requirements and payload capacity. The authors also discuss challenges such as detection and data loss during extraction.

SYSTEM ARCHITECTURE

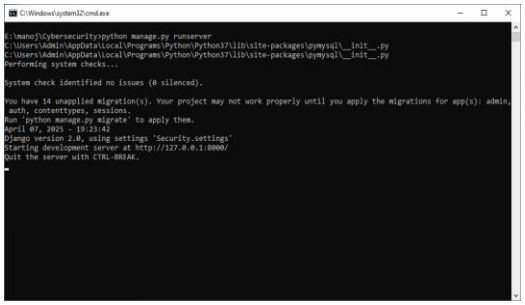


IMPLEMENTATION

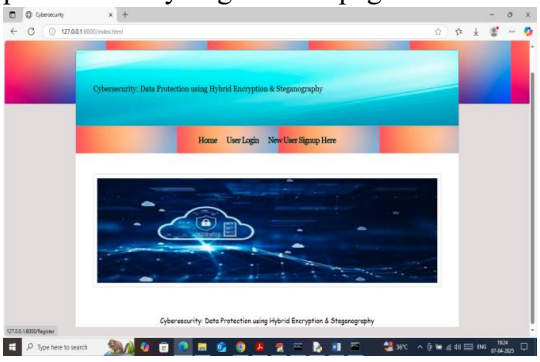
SCREEN SHOTS

To run project install python 3.7.2 and then install all packages given in requirements.txt file. Install MYSQL and then copy content from 'database.txt' file and paste in MYSQL console to create database.

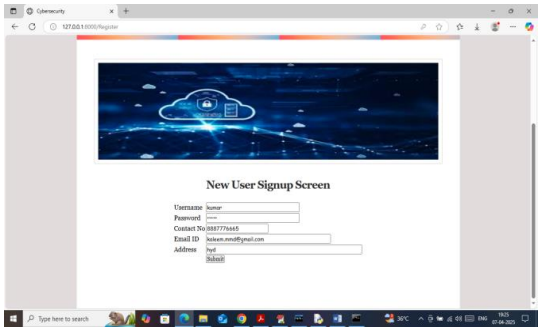
Now double click on 'run.bat' file to start python web server and then will get below page



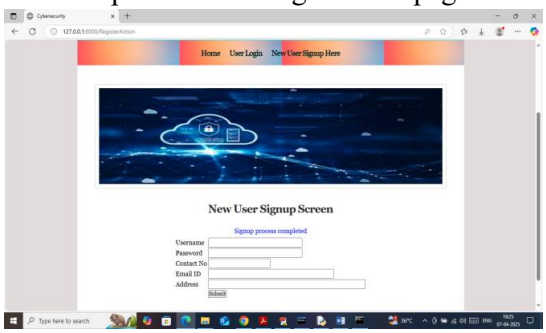
In above screen python server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and then press enter key to get below page



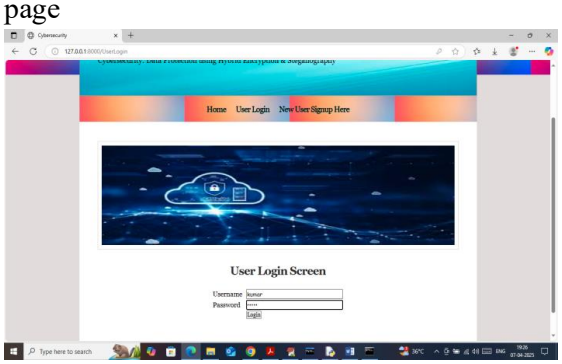
In above screen click on 'New User Sign up' link to get below page



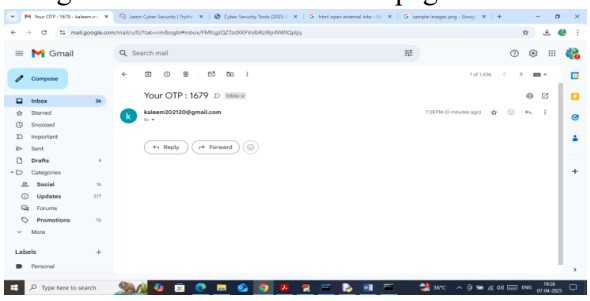
In above screen user is entering sign up details and then press button to get below page



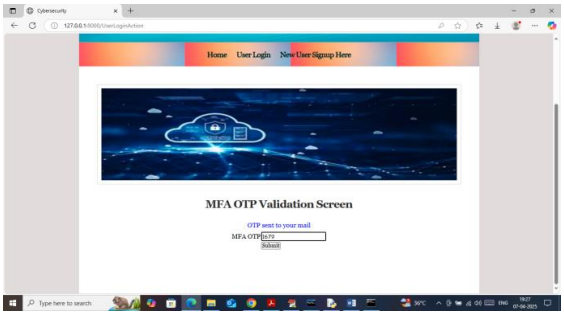
In above screen sign up process completed and now click on 'User Login' link to get below page



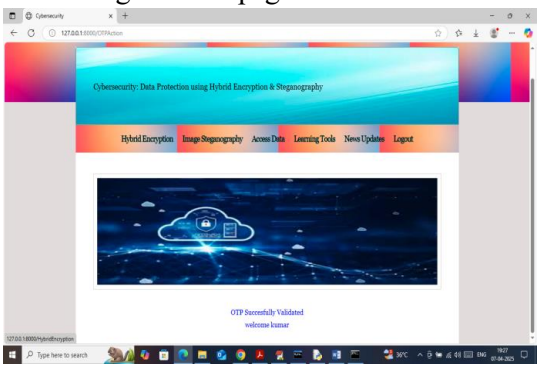
In above screen user is login and after login will get OTP in email like below page



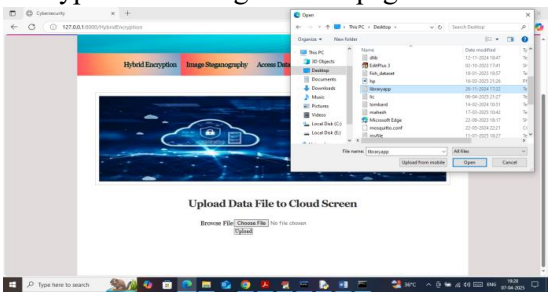
In above screen OTP received to email and enter to application to continue authentication process



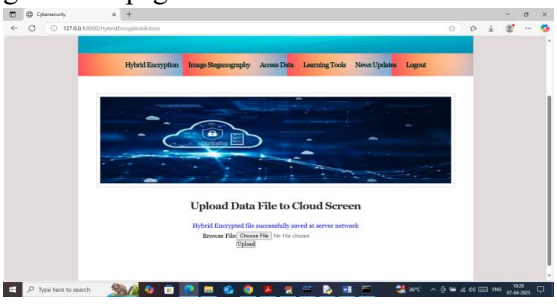
In above screen enter OTP and then press button to get below page



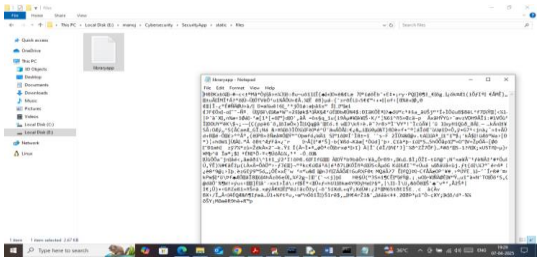
In above screen user can click on 'Hybrid Encryption' link to get below page



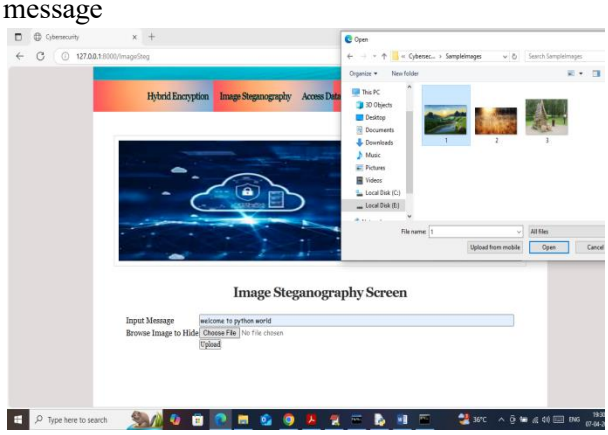
In above screen select and upload any file and then click on 'Open and upload' buttons to saved file in encrypted format and then will get below page



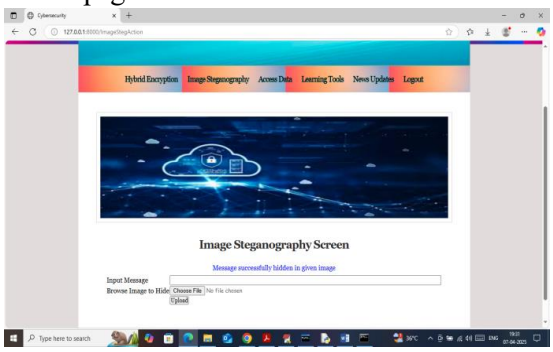
In above screen can see file saved at server and in below screen can see file content in encrypted format



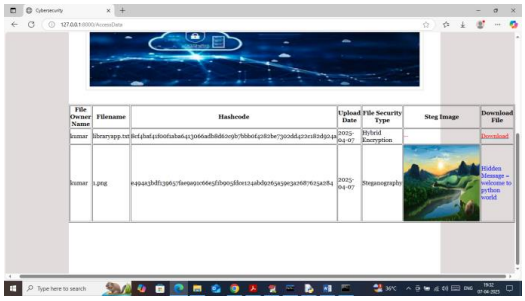
In above screen can see file content is in very heavy encrypted format and now go back and click on 'Image Steganography' link to hide message



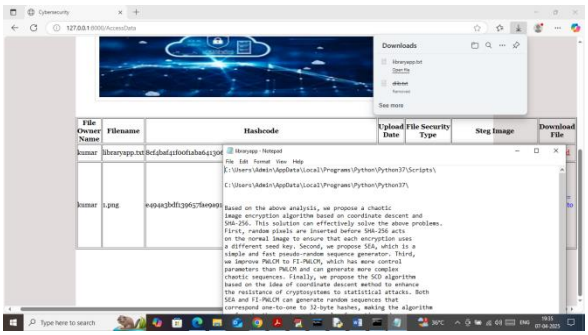
In above screen in text field I entered some message to hide and then selecting and uploading image and then press buttons to get below page



In above screen can see message successfully hidden in image and similarly you can upload and test any number of files. Now click on 'Access Data' link to access past uploaded files



In above screen can see all uploaded files along with Hashcode and encryption type as 'Steganography or Hybrid'. If encryption type 'Steganography' then system will display image along with 'Extracted hidden message in blue text'. If encryption type is 'Hybrid Encryption' then user can click on red 'Download' link download file in decrypted format



In above screen can see file is downloaded in decrypted format and can see decrypted text. Similarly you can upload and download any number of files and now click on 'Learning Tools' link to learn about tools

In above screen can learn about tools and now click on 'News Updates' to get below page

In above screen user can read latest news on Cybersecurity.

So by using above applications you can secured data with Steganography and Hybrid encryption.

CONCLUSION

The proposed system on Cybersecurity: Data Protection Using Hybrid Encryption and Steganography provides a secure and reliable method for protecting sensitive digital information from unauthorized access and cyber threats. By combining the strengths of hybrid encryption techniques with steganography, the system ensures both confidentiality and invisibility of the data during transmission. Hybrid encryption offers strong security through the integration of symmetric and asymmetric cryptographic algorithms, while steganography conceals the existence of the encrypted data within digital media files such as images or audio.

This dual-layer security approach significantly reduces the risk of data interception, hacking, and information leakage. The system also improves authentication, integrity, and privacy, making it suitable for applications in banking, healthcare, military communication, and cloud storage environments. Experimental analysis demonstrates that the proposed model achieves efficient encryption performance with enhanced security compared to traditional methods.

Overall, the integration of encryption and steganography provides an advanced cybersecurity solution capable of safeguarding confidential information in modern digital communication systems. Future improvements can focus on increasing embedding capacity, reducing processing time, and incorporating artificial intelligence techniques for smarter threat detection and adaptive security mechanisms.

FUTURE WORK

Future enhancements to the proposed cybersecurity system can focus on improving security efficiency, scalability, and adaptability against emerging cyber threats. Advanced cryptographic algorithms with lower computational complexity can be integrated to increase encryption speed while maintaining strong security. Artificial Intelligence and Machine Learning techniques may also be incorporated to detect suspicious activities, identify intrusion attempts, and provide real-time threat analysis.

The steganography module can be further enhanced by developing adaptive data hiding techniques that increase embedding capacity without affecting the quality of the cover media. Future systems may also support multimedia steganography using video, audio, and 3D files for higher security and larger data transmission. In addition, cloud-based implementation can be explored to provide secure remote storage and communication services for organizations and individuals.

Blockchain technology can also be integrated to ensure tamper-proof data sharing and decentralized security management. Furthermore, the proposed model can be optimized for mobile and IoT devices to provide lightweight and energy-efficient protection in smart environments. These advancements will help create a more intelligent, scalable, and robust cybersecurity framework capable of handling future digital security challenges effectively.

REFERENCE

1. , *Cryptography and Network Security: Principles and Practice*, Pearson Education, 7th Edition, 2017.
2. Behrouz A. Forouzan, *Data Communications and Networking*, McGraw-Hill Education, 5th Edition, 2013.
3. Neil F. Johnson and Sushil Jajodia, “Exploring Steganography: Seeing the Unseen,” *Computer Journal*, Vol. 31, No. 2, pp. 26–34, 1998.
4. Adi Shamir, Ron Rivest, and Leonard Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, 1978.
5. Joan Daemen and Vincent Rijmen, “The Design of Rijndael: AES – The Advanced Encryption Standard,” Springer, 2002.
6. National Institute of Standards and Technology, “Advanced Encryption

Standard (AES)," FIPS PUB 197, 2001.

7. Jessica Fridrich, "Applications of Data Hiding in Digital Images," Proceedings of the International Conference on Information Technology, 2000.
8. Menezes, Van Oorschot, and Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
9. IEEE, "Security and Privacy in Cybersecurity Systems," IEEE Digital Library, 2021.
10. ACM, "Recent Trends in Hybrid Encryption and Secure Data Communication," ACM Journals, 2022.