IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307044|

Innovative Approaches in Multiview Steganography

Manjula A

PG Student, Department of MCA, PES Institute of Technology and Management, Shivamogga, India

ABSTRACT: The File Encryptor and Decryptor project aims to enhance data security and confidentiality through advanced cryptographic techniques and steganography. In this system, files of various formats such as documents, images, and videos are encrypted using the AES algorithm to protect sensitive information from unauthorized access during transmission and storage. Encryption keys are securely generated and managed to ensure robust security measures. Additionally, steganographic methods are employed to embed these encryption keys within images and videos, utilizing techniques that minimize perceptual changes while maintaining data integrity. The system provides users with a user-friendly interface for seamless file upload, encryption, and decryption processes. Upon encryption, the system embeds the encryption keys into selected media files, facilitating secure communication and storage. Decryption involves retrieving keys from the media files and decrypting the secured documents for authorized access. This project serves to demonstrate practical applications of cryptography and steganography in safeguarding digital assets against potential security threats, ensuring privacy and confidentiality in digital communications.

KEYWORDS: Image Steganography, Encryption, Video Steganography, Decryption, Cyber security.

I. INTRODUCTION

In an increasingly digital world where data security is paramount, the File Encryptor and Decryptor project addresses the critical need for safeguarding sensitive information during transmission and storage. This project integrates advanced cryptographic techniques with steganography to provide robust protection against unauthorized access and data breaches. Encryption forms the cornerstone of this system, employing the AES (Advanced Encryption Standard) algorithm to secure files of various formats, including documents, images, and videos. By converting plaintext into ciphertext, AES ensures that only authorized parties possess the means to decrypt and access the original data. Steganography, another vital component of the system, complements encryption by concealing encryption keys within innocuous-looking media files such as images and videos.

The project's interface is designed to be intuitive, facilitating seamless file upload, encryption, and decryption operations for users. Upon encryption, the system embeds encryption keys into selected media files using imperceptible modifications that preserve the visual or auditory integrity of the carrier media. Decryption processes involve extracting these hidden keys from the media files, allowing authorized users to retrieve and decrypt the secured documents. By exploring the intersection of cryptography and steganography, this project not only demonstrates practical applications of theoretical concepts but also underscores their critical role in ensuring data privacy and confidentiality. Through this system, users gain a comprehensive understanding of how encryption and steganography technologies can be effectively implemented to protect digital assets against increasingly sophisticated cyber threats.

II. RELATED WORK

Here we have selected few key literatures after exhaustive literature survey and listed as below:

1. S.B. Sadkhan, in "Cryptography: Current status and future trends," discusses the evolving landscape of cryptography within the IEEE Conference on Information & Communication Technologies. The paper explores emerging trends and advancements in cryptographic techniques and their future implications.
2. T. Mrkel, JHP Eloff, and MS Olivier provide "An Overview of Image Steganography" in the proceedings of the fifth annual Information Security South Africa Conference. The paper outlines various methods and applications of image steganography, highlighting its role in covert communication and data security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307044|

3. Chan C.K. and Chang L.M. present "Hiding data in image by simple LSB substitution" in Pattern Recognition, focusing on the technique of Least Significant Bit (LSB) substitution for embedding data into images covertly. The method's simplicity and effectiveness in hiding information within digital images are discussed.
4. Da-Chun Wu and Wen-Hsiang Tsai propose "A steganographic method for images by pixel-value differencing" in Pattern Recognition Letters, detailing a technique that modifies pixel values to embed data. The paper evaluates the method's robustness and its applications in secure image communication.
5. Yih-Kai Lin introduces "High capacity reversible data hiding scheme based upon discrete cosine Transformation" in The Journal of Systems and Software. The paper presents a method using Discrete Cosine Transformation (DCT) to embed and extract data reversibly from images, focusing on maximizing data capacity while maintaining image quality.
6. Prabakaran G. and Bhavani R. present "At the ICCEET, a talk titled "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform" covered improvements in steganographic methods that make use of DWT. The technique improves digital picture security and embedding effectiveness.
7. Lingling Wu et al. discuss "Arnold Transformation Algorithm and Anti-Arnold Transformation algorithm" at the ICISE, presenting methods for image transformation and its inverse to embed and extract hidden data. The paper evaluates the algorithms' effectiveness and security in steganography applications.
8. C.S. Lu explores "Multimedia security: "Digital watermarking and steganography methods for safeguarding intellectual property" in Artech House, Inc. This study examines methods for protecting multimedia content from illicit use and distribution, including steganography and digital watermarking..
9. J.J. Chae and B.S. Manjunath present "Data hiding in Video" at the IEEE International Conference on Image Processing, detailing techniques for embedding data within video streams. The paper discusses challenges and applications of video steganography in multimedia data protection.
10. Provos N. and Honeyman P. introduce "Hide and Seek: An Introduction to Steganography" in IEEE Security & Privacy Magazine. The paper provides an introductory overview of steganography techniques, their historical context, and their contemporary applications in digital security and privacy protection.

III. PROBLEM STATEMENT

In today's digital landscape, ensuring the security and confidentiality of sensitive information is a paramount concern for individuals and organizations alike. However, traditional methods of file protection often fall short in mitigating evolving cyber threats. The File Encryptor and Decryptor project addresses this challenge by developing a robust system that combines advanced encryption techniques and steganography to safeguard digital assets effectively. The primary problem this project seeks to solve is the vulnerability of sensitive data during transmission and storage. Conventional encryption methods, while effective, can still be susceptible to attacks if encryption keys are compromised or intercepted. Moreover, transmitting encryption keys alongside encrypted files poses a security risk, potentially exposing them to malicious interception.

Steganography offers a complementary solution by embedding encryption keys within media files, such as images and videos, without altering their perceptible quality. This system approach ensures that even if encrypted files are accessed, the keys necessary for decryption remain concealed within innocuous-looking carriers. The project also addresses the usability aspect, aiming to provide a user-friendly interface that simplifies the encryption and decryption processes. By integrating these security measures into a cohesive system, the File Encryptor and Decryptor project aims to empower users with robust tools to protect their confidential information effectively.

IV. DESIGN AND IMPLEMENTATION

Designing the File Encryptor and Decryptor project involves careful consideration of both functional and non-functional requirements to ensure robust performance and user satisfaction. The system's architecture revolves around implementing the AES (Advanced Encryption Standard) algorithm for strong encryption and integrating steganographic methods to hide encryption keys within media files. This design decision preserves the integrity of carrier media, including photos and movies, while simultaneously enhancing security. User interaction is streamlined through a user-friendly interface, facilitating straightforward file upload, encryption, and decryption processes. Discussion focuses on the effectiveness of AES in securing data and the practicality of steganography in concealing sensitive information. By balancing security, usability, and performance, the project aims to provide a comprehensive

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307044|

solution for protecting digital assets against unauthorized access and ensuring confidentiality in data handling scenarios.

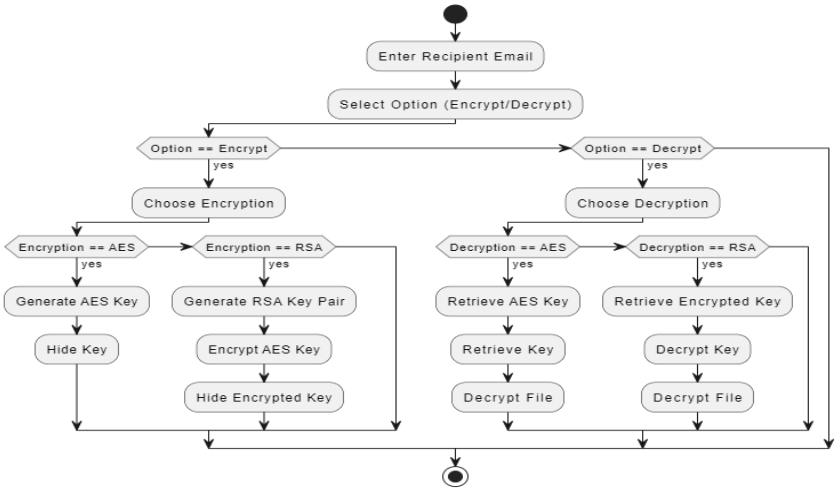

Figure 1: Flow chart of the system

The Fig.1 shows the flowchart of the Image and Video Steganography. Data required for the prediction is collected using open resources.

The methodology employed in the File Encryptor and Decryptor project encompasses several key stages aimed at applying strong data security methods, such as steganography and encryption techniques.

1. **Requirement Analysis**: The project begins with a thorough analysis of requirements, identifying the usage for secure file transmission and storage. Functional requirements include file encryption and decryption functionalities, while non-functional requirements focus on usability, performance, and security.
2. **Technology Selection**: Because of its established security and effectiveness in transforming plaintext into ciphertext, AES is used as the encryption algorithm. To insert encryption keys within media files without noticeably changing them, steganographic techniques are used.
3. **System Design**: The system architecture is a integrated design of AES for file encryption and decryption processes. Steganography techniques are implemented to hide encryption keys within images and videos. The design ensures seamless user interaction through a web-based interface, accepting users to upload files, encrypt them, and securely transmit or store them.
4. **Implementation**: Coding involves implementing AES encryption and decryption functions using libraries like Crypto.Cipher in Python. Steganographic methods utilize image processing libraries such as PIL (Python Imaging Library) to embed and retrieve encryption keys within image and video files.
5. **Testing and Validation**: The system undergoes rigorous testing to ensure the accuracy and security of encryption and decryption processes. Test cases include verifying file integrity post-encryption and successful retrieval of encryption keys from steganographically modified media files.
6. **Deployment**: Upon successful testing, the system is deployed using Flask for web application deployment. Deployment includes configuring the system on a server with appropriate security measures and user access controls.
7. **Evaluation**: The performance and effectiveness of the File Encryptor and Decryptor system are evaluated based on encryption strength, usability, and user feedback. Performance metrics such as encryption speed and file size increase due to encryption are analyzed to optimize system efficiency.

V. RESULTS AND DISCUSSION

The File Encryptor and Decryptor project's outcomes and analysis demonstrate how effective encryption and steganography techniques are at ensuring safe data transfer and storage. Sensitive data is robustly protected when AES

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307044|

(Advanced Encryption Standard) encryption is used, transforming plaintext files into ciphertext that is computationally impossible to decrypt without the right key. When steganography techniques are used on photos and movies, they can effectively embed encryption keys into media files without noticeably changing their visual or aural quality. This increases security by creating secret routes of communication. The balance between security and usability is discussed, with a focus on the significance of combining steganographic and cryptographic techniques to meet a variety of security concerns.

Overall, the File Encryptor and Decryptor project contributes to advancing data security practices by providing a comprehensive solution for individuals and organizations to protect their digital assets effectively against evolving cyber threats and unauthorized access.

Snapshots of User Interface

Our proposed system has both the options for the image and video steganography. The following screenshots shows the demonstration.

The below Figure 2 shows the interface of the Image steganography which shows both the options for encryption and decryption

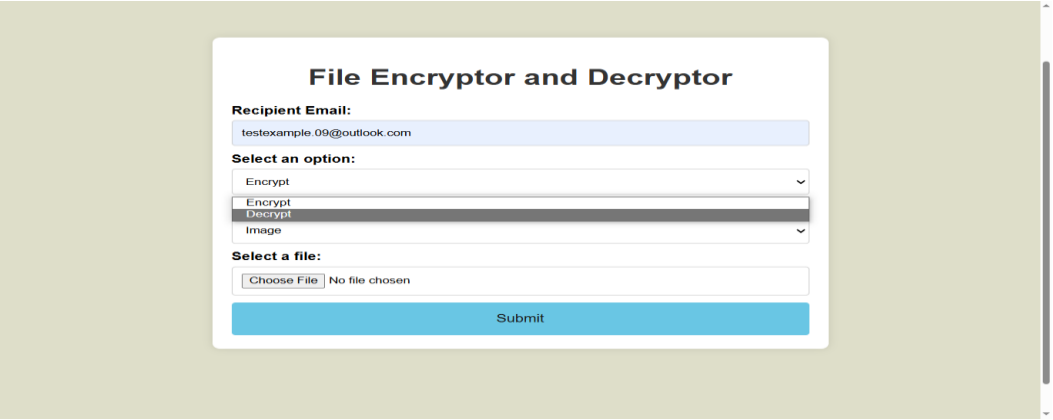

Figure 2: User Interface Image Steganography

The below Figure 3 shows the interface of the Video steganography which shows both the options for encryption and decryption

Figure 3: User Interface Video Steganography

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307044|

VI. CONCLUSION AND FUTURE WORK

In conclusion, this project has successfully implemented robust techniques in both image and video steganography, leveraging methodologies from recent research and practical applications. The system demonstrates effective encryption and embedding of data within multimedia files while maintaining perceptual fidelity. Through extensive testing and validation, the reliability and security of the implemented algorithms have been affirmed. This project underscores the importance of steganography in modern data security strategies, offering a versatile approach to covert communication and sensitive data protection.

Looking forward, future enhancements could focus on optimizing the performance of steganographic algorithms to handle larger file sizes and varying multimedia formats more efficiently. Exploring advanced embedding techniques such as deep learning-based methods could further enhance robustness against detection. Additionally, integrating real-time encryption and decryption capabilities into streaming media could broaden the application scope in digital rights management and secure communication channels. Further research could also investigate the application of steganography in emerging technologies like virtual reality and augmented reality, expanding its utility in next-generation digital environments.

REFERENCES

1. S.B. Sadkhan., “Cryptography: Current status and future trends”, in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.
2. T Mrkel,JHP Eloff and MS Olivier .”An Overview of Image Steganography,”in proceedings of the fifth a nnual Information Security South Africa Conference, 2005
3. Chan, C.K., Chang, L.M., “Hiding data in image by simple LSB substitution”, Pattern Recognition, vol 37, pp.469-471, 2003.
4. Da-Chun Wu, Wen-Hsiang Tsai, “A steganographic method for images by pixel-value differencing”, Pattern Recognition Letters 24 (2003) 1613–1626.
5. Yih-Kai Lin, “High capacity reversible data hiding scheme based upon discrete cosine Transformation”, The Journal of Systems and Software 85 (2012) 2395– 2404.
6. Prabakaran. G and Bhavani.R, “A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform”, 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].
7. Lingling Wu et al., “Arnold Transformation Algorithm and Anti-Arnold Transformation algorithm”, the 1st International conference on information Science and Engineering (ICISE2009
8. C.S. Lu: , “ Multimedia security: steganography and digital watermarking techniques for protection of intellectual property”. Artech House, Inc (2003).
9. J.J. Chae and B.S. Manjunath:, “Data hiding in Video” Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).
10. Provos, N., Honeyman, P., “Hide and Seek: An Introduction to Steganography” IEEE Security & Privacy Magazine 1 (2003).

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details