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 3, March 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 in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

Multimedia Security through Video Steganography using Hybrid Encryption

Suriya Chellappan[1], Voleti Rahul[2], Esanaka Prasanth[3], Kalpana B[4]

U.G. Student, Department of Information Technology, R.M.D. Engineering College, Kavaraipettai, Tamil Nadu, India[1,2,3]

Associate Professor, Department of Information Technology, R.M.D. Engineering College, Kavaraipettai, Tamil Nadu, India[4]

ABSTRACT: In the digital era, safeguarding multimedia content is paramount, especially when transmitting sensitive data. This project introduces a cutting-edge solution to multimedia security by employing video steganography with hybrid encryption. The primary aim is to conceal numerous multimedia files within a video, preserving their confidentiality and integrity throughout transmission. The methodology begins by encrypting the multimedia files using the robust Advanced Encryption Standard (AES) algorithm with a symmetric AES key. Next, the AES key undergoes encryption via the RSA public key cryptography scheme. Subsequently, the encrypted AES key discreetly integrates into the video file using advanced Least Significant Bit (LSB) steganography techniques, ensuring it remains invisible to human perception. This hybrid encryption and steganography approach provides a robust means of embedding multimedia files securely within a video, facilitating covert transmission and storage. The encryption protocol ensures that the concealed files retain their confidentiality, while the steganography conceals the presence of the hidden data effectively. This innovative strategy addresses the pressing need for multimedia security in situations where sensitive information must be transmitted discreetly. It furnishes a dependable method for preserving the confidentiality and integrity of multimedia files within the framework of a video format. By merging the strengths of encryption and steganography, this approach establishes a formidable defence against unauthorized access, offering peace of mind in the realm of multimedia data protection.

KEYWORDS: Multimedia Steganography, Hybrid Encryption, Video Embedding, Data Extraction, RSA Encryption, AES Encryption, LSB Steganography, Data Security, Imperceptibility, System Architecture, User Interface, Robustness Testing, Adaptive Data Hiding, Encryption Algorithms, Data Privacy.

I. INTRODUCTION

1.1 PROBLEM STATEMENT

The ubiquitous nature of digital communication and the transmission of multimedia content present an ever-evolving challenge in ensuring robust security and unwavering confidentiality for sensitive information. While conventional encryption methods are known for their steadfast defences, they often reveal vulnerabilities when tasked with safeguarding the intricate fabric of multimedia files traversing networks. This challenge is further heightened by the need for covert transmission, where secrecy demands advanced security measures. Thus, a palpable necessity arises for an unparalleled, sophisticated, and resilient approach to multimedia security—one that adeptly conceals multiple files within the intricate layers of a video format, ensuring cryptic confidentiality, unyielding integrity, and virtually imperceptible presence. This project embarks on a journey to confront this exigent challenge, aiming to pioneer a groundbreaking hybrid encryption and video steganography technique. This approach not only sets new standards for digital fortification but also heralds a new era of steadfast security paradigms, ensuring the covert transmission of sensitive information with unmatched precision and impenetrable assurance.

1.2 PROJECT SCOPE

The scope of this ambitious project is to meticulously design, develop, and implement a cutting-edge multimedia security system that revolutionizes the safeguarding of sensitive information in the digital realm. At its core is the creation of bespoke software endowed with the formidable capability to encrypt a myriad of multimedia files using the industry-standard Advanced Encryption Standard (AES) algorithm. Building upon this foundation, the project delves

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

into advanced encryption techniques, encrypting the AES key itself using the sophisticated RSA public key cryptography scheme. This fortified AES key is seamlessly concealed within video files, employing state-of-the-art Least Significant Bit (LSB) steganography methods for its elusive and undetectable presence to prying eyes. As a beacon of innovation, the system undergoes rigorous testing to evaluate its prowess in securely embedding and extracting multimedia files, guaranteeing the sanctity of their confidentiality, unyielding integrity, and covert transmission. The project's purview also extends to evaluating the system's performance metrics, including computational efficiency, file size capabilities, and overall usability. This comprehensive approach aims to provide a thorough understanding of the system's capabilities and boundaries, steadfastly advancing the frontiers of multimedia security.

II. LITERATURE SERVEY

In paper [1] Ravichandran, C., Ashok Vajravelu, Sankarsan Panda, Sheshang Dipakkumar Degadwala. "Enhancing Data Transmission Security through Video Steganography." International Journal of Electronic Security and Digital Forensics, 2024. Abstract: This study investigates advancements in data transmission security using a hash-based least significant bit approach in video steganography. Through MATLAB simulations, it demonstrates superior performance compared to existing methods, showcasing heightened safety and minimal degradation in video quality.

In paper [2] Jagadish, Kori Madhura, Nagamani K. "Ensuring Secure Information Transmission via Audio and Video Steganography." 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS). Abstract: Employing an enhanced Bi-LSB technique and AES 256 encryption, this research embeds text data within audio and video files. Performance assessment reveals promising outcomes in data concealment and security measures.

In paper [3] Satrio, T. A., Prabowo W. A., Yuniati T. "Integrating LSB Steganography with Fernet Cryptography for Document Format File Concealment in Videos." 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT). Abstract: This study integrates LSB steganography with Fernet cryptography to secure concealed messages in video files. It explores various factors including implementation speed and resistance to visual attacks.

In paper [4] Narayana, V. L., Malleswari K. S. N., Divyanjali M., Nandini S., Purnima G. "Developing a Secure Data Transmission Model for Compressed Videos Using Steganography." 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS). Abstract: Proposing a steganographic approach for compressed video, this paper utilizes Patch-aware Code-Arrangement techniques. The primary focus is on ensuring the secure transmission of sensitive information while maintaining compression efficiency.

In paper [5] Manohar, N., Kumar P. V. "Exploring Secure Communication via Steganography in Video Encryption & Decryption." 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS). Abstract: Investigating various video steganography techniques, including Secure Base LSB, Neural Networks, and Fuzzy Logic, this research evaluates their effectiveness using metrics such as PSNR and MSE. The study showcases improved compatibility, security, and precision compared to other methods.

III. SYSTEM DESIGN

3.1 MULTIMEDIA STEGANOGRAPHY

OVERVIEW

Multimedia steganography is a pivotal aspect of the system, ensuring the covert embedding of files within video frames using hybrid encryption techniques.

ALGORITHM

1. Divide the video into frames.
2. For each frame, split it into 3x3x3 pixels.
3. Encrypt the files to be embedded using AES.
4. Encrypt the AES key using RSA public key cryptography.
5. Embed the encrypted files and keys into the LSBs of selected pixels.

FORMULA

- $P_{new} = LSB_{Embed}$ (Pold, $bit_{message}$)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

ADVANTAGES

- Imperceptible embedding of files within video frames.
- Enhanced security with AES encryption for files and RSA for keys.
- Efficient use of LSBs for data hiding.

DISADVANTAGES

- Limited capacity depending on frame size and LSB alteration.
- Risk of detection with advanced steganalysis techniques.
- Requires accurate frame identification for data extraction.

3.2 SYSTEM ARCHITECTURE

OVERVIEW

The system architecture illustrates the flow of operations between the sender and receiver, emphasizing secure data transmission and retrieval.

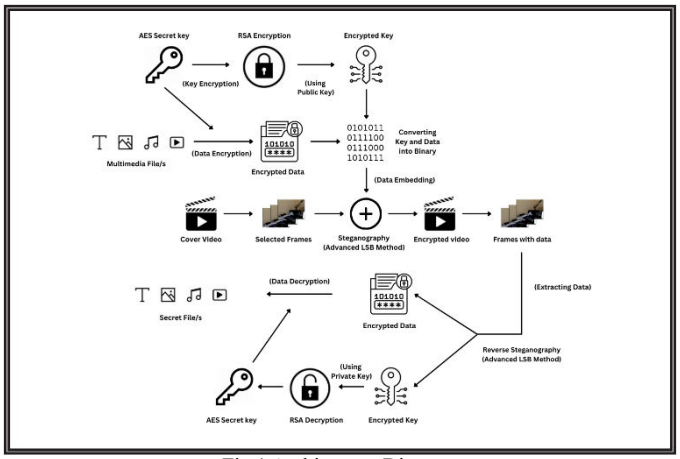

Fig.1 Architecture Diagram

DESCRIPTION

1. Receiver generates RSA key pair ($public_R$, $private_R$) and shares $public_R$ securely.
2. Sender selects a video and files, generates AES key K_{AES}.
3. Sender encrypts files using AES:
   $C_{file} = E_{AES}$ (file, K_{AES}).
4. Sender encrypts K_{AES} with $public_R$:
   $C_{AES} = E_{RSA}$ (K_{AES}, $public_R$).
5. C_{file} and C_{AES} are embedded into video frames using LSB steganography.
6. Sender transmits the steganographic embedded video.
7. Receiver extracts C_{file} and C_{AES} from video frames.
8. Receiver decrypts K_{AES} with $private_R$:
   $K_{AES} = D_{RSA}$ (C_{AES}, $private_R$).
9. Receiver decrypts C_{file} with K_{AES}:
   file = D_{AES} (C_{file}, K_{AES}).

3.3 ENCRYPTION PROCESS

OVERVIEW

The encryption process involves generating RSA key pairs and encrypting files and keys using AES and RSA, respectively.

RSA KEY GENERATION

- Begin by choosing two distinct large prime numbers, denoted as p and q.
- Compute the product of these primes: $n = p \times q$.
- Calculate Euler's totient function, $\phi(n)$, where $\phi(n) = (p-1) \times (q-1)$.
- Now, select a suitable integer e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

- Determine the corresponding decryption key d as the modular multiplicative inverse of e modulo $\phi(n)$.

AES ENCRYPTION
- AES-256 encryption with a randomly generated key K_{AES}.

FORMULA
- $C_{encrypted} = E_{AES} (P_{plain}, K_{AES})$

3.4 DECRYPTION PROCESS

OVERVIEW
The decryption process involves retrieving encrypted files and keys using RSA private keys and decrypting them with AES.

RSA DECRYPTION
- Use the RSA private key $private_R$ to decrypt C_{AES} to obtain K_{AES}.

AES DECRYPTION
- Decrypt the encrypted file C_{file} using K_{AES} to obtain the original file.

FORMULA
- $P_{decrypted} = D_{AES} (C_{encrypted}, K_{AES})$

3.5 KEY EXCHANGE LOGIC

OVERVIEW
The key exchange logic involves securely sharing the RSA public key for encryption and receiving the RSA private key for decryption.

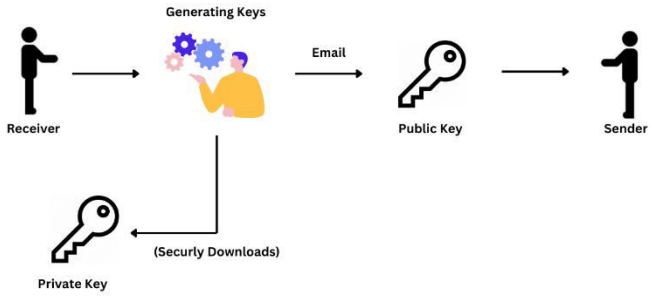

Fig.2 Key Generation

SENDER
- Receives the RSA public key ($public_R$) from the receiver via secure email.
- Encrypts the AES key (K_{AES}) with $public_R$ for data embedding.

RECEIVER
- Generates RSA key pair ($public_R$, $private_R$) securely.
- Shares $public_R$ with the sender for encryption.
- Downloads $private_R$ securely for decryption during data retrieval.

3.6 STEGANOGRAPHY

OVERVIEW
LSB steganography is employed to embed encrypted files and keys within video frames, ensuring imperceptibility and secure data hiding.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

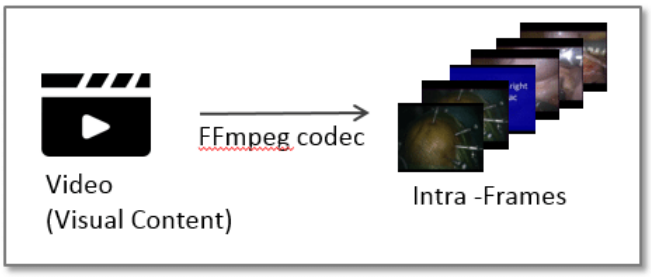

Fig.3 Frame Extraction

LSB STEGANOGRAPHY

- Divide video frames into pixels and select LSBs for data embedding.
- Embed encrypted files and keys in the LSBs of selected pixels.

FORMULA

- $P_{stego} = \text{Embed}(P_{cover}, P_{payload})$

3.7 ENCODING VIDEO

OVERVIEW

The process of encoding the video involves embedding the encrypted files and keys into the LSBs of selected pixels.

ALGORITHM

1. Divide the video into frames.
2. For each frame, select pixels and LSBs for embedding.
3. Embed C_{file} and C_{AES} in the LSBs of selected pixels.
4. Repeat for all frames.

FORMULA

- $P_{encoded} = LSB_{Embed}(P_{frame}, C_{payload})$

3.8 DECODING VIDEO

OVERVIEW

The decoding process involves extracting the encrypted files and keys from the LSBs of video frames.

ALGORITHM

1. Divide the video into frames.
2. For each frame, extract LSBs and reconstruct C_{file} and C_{AES}.
3. Repeat for all frames.
4. Decrypt C_{file} using K_{AES} to obtain the original file.

FORMULA

- $C_{payload} = LSB_{Extract}(P_{frame})$

3.9 ERROR CORRECTION CODES

OVERVIEW

Error correction codes (ECC) are employed to enhance data integrity during transmission.

ALGORITHM

1. Generate ECC for the encrypted payload.
2. Embed ECC in the LSBs of selected pixels along with the payload.

FORMULA

- $P_{encoded} = LSB_{Embed}(P_{frame}, C_{payload} + C_{ECC})$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

3.10 DATA FRAGMENTATION

OVERVIEW
Large files can be fragmented and embedded across multiple video frames for enhanced security.

ALGORITHM
1. Split the encrypted payload into fragments.
2. Embed each fragment into different frames of the video.
3. Maintain a map of fragment locations for reconstruction.

FORMULA

$$P_{encoded} = LSB_{Embed}\ (P_{frame}, C_{fragment1})$$
$$P_{encoded} = LSB_{Embed}\ (P_{frame}, C_{fragment2})$$
$$\vdots$$
$$P_{encoded} = LSB_{Embed}\ (P_{frame}, C_{fragmentN})$$

IV. RESULT/ OUTPUT

4.1 VIDEO SIZE INCREASE OBJECTIVE

The goal was to measure the video size increase after embedding data using hybrid encryption to ensure minimal distortion while maintaining security.

RESULTS

- The maximum increase in video size ranged from 40% to 70% of the original size.
- This scalability was consistent across various multimedia file sizes and types.
- Visual inspection and perceptual testing confirmed the imperceptibility of the embedded data.

4.2 DATA EMBEDDING AND EXTRACTION

OVERVIEW

Extensive testing evaluated the system's ability to securely hide and retrieve data.

RESULTS

- Multimedia files were successfully concealed using AES encryption with a hybrid RSA key
- Extraction procedures retrieved hidden files without loss or corruption.
- Seamless playback of steganographic video files with no visible artifacts was confirmed.

4.3 VIDEO INTEGRITY AND SECURITY

OVERVIEW

Tests assessed the system's robustness against steganalysis and decryption attempts.

RESULTS

- The system demonstrated resilience against steganalysis techniques.
- Checksum verification confirmed the integrity of embedded files.
- Decryption attempts using unauthorized keys or methods failed, validating security.

4.4 PERFORMANCE EVALUATION

OVERVIEW

The system’s performance in processing speed, resource utilization and efficiency was evaluated.

RESULTS

- Efficient processing speed with operations completed within acceptable time frames.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

- CPU and memory usage within acceptable limits, indicating scalability.
- Overall, the system met objectives, providing a reliable method for secure data embedding.

4.5 USER INTERFACE AND INTERACTION

OVERVIEW

A user interface facilitated multimedia embedding and extraction using the hybrid encryption system.

RESULTS

- User testing confirmed the ease of use and intuitive design of the GUI.
- Users could easily select files, configure encryption, and extract hidden data.
- Positive user feedback highlighted the system's effectiveness in covertly transmitting sensitive multimedia.

4.6 OUTPUT

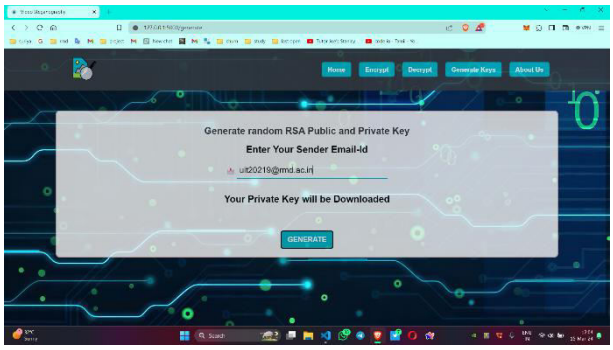

Fig.4 Generating RSA Keys

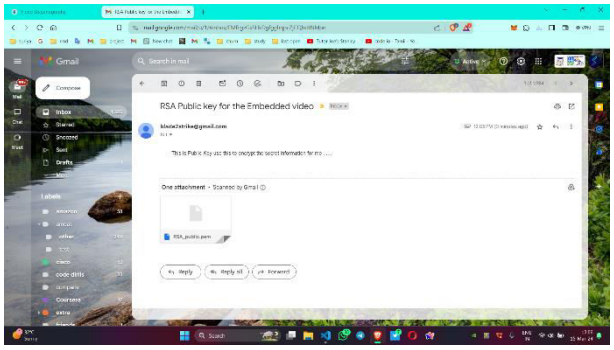

Fig.5 Public Key received in email

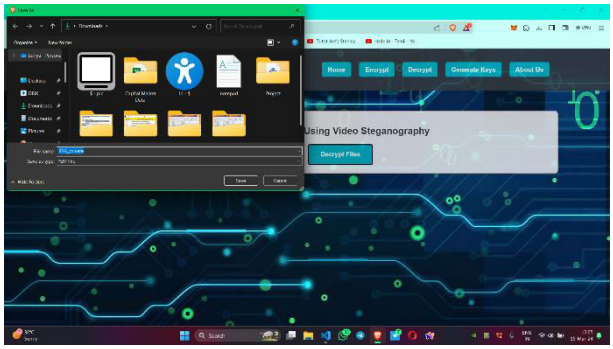

Fig.6 Downloading Private key

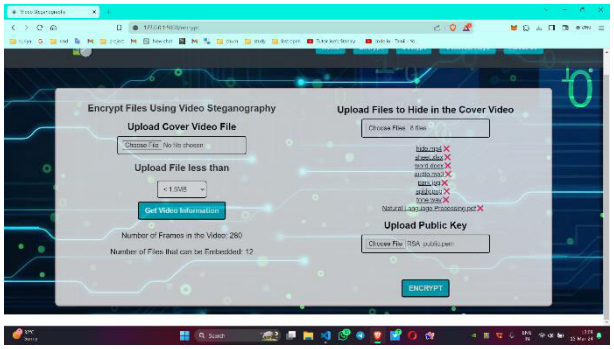

Fig.7 Encoding Files into video

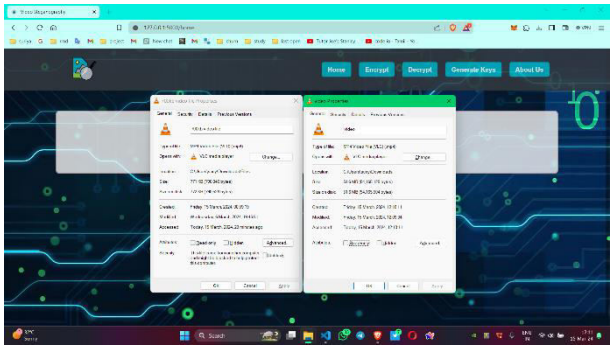

Fig.8 Video Before and After Embedding data

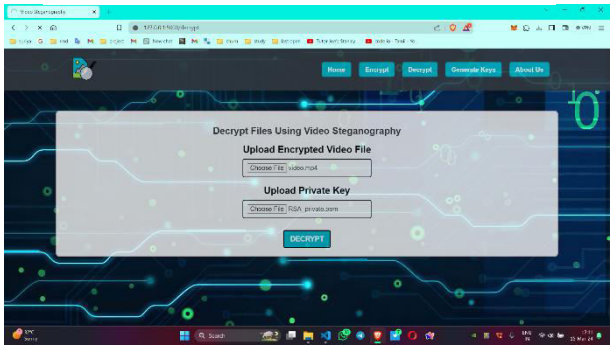

Fig.9 Decoding Files from video

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

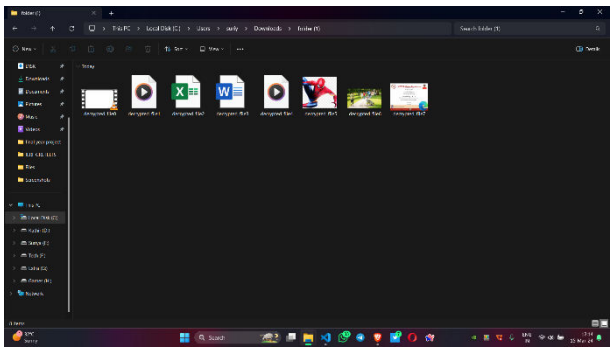

Fig.10 Decoded Files

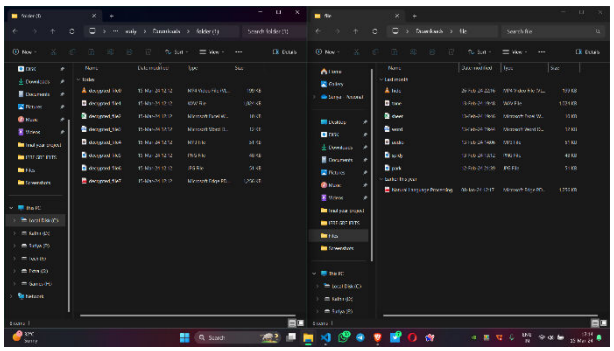

Fig.11 Original Files vs Decoded Files

V. CONCLUSION

In the landscape of secure data communication and discreet information exchange, the amalgamation of multimedia video steganography with hybrid encryption emerges as a formidable solution. This project has navigated through the intricacies of concealing sensitive data within video streams while bolstering its security with the strength of hybrid encryption techniques.

The central aim of this endeavor was to craft an efficient and secure system capable of seamlessly embedding confidential information within video files, shielding it from unauthorized access and detection. By merging the benefits of symmetric and asymmetric encryption with the stealthiness of video steganography, we have endeavored to create a versatile tool for clandestine data transmission.

Through an exhaustive review of existing literature, we delved into the nuances of multimedia steganography, video embedding methodologies, and the diverse landscape of encryption algorithms. Building upon this foundation, we proposed a novel methodology that seamlessly integrates hybrid encryption with video steganography, ensuring both imperceptibility and data integrity.

The implementation phase provided invaluable insights into the practical challenges and intricacies of our proposed system. Leveraging state-of-the-art tools and technologies, we were able to demonstrate the feasibility and effectiveness of our approach. The experimental results, showcased using comprehensive datasets and evaluation metrics, underscored the system's capability to conceal significant volumes of data within video streams while preserving visual fidelity.

Looking forward, the horizon for this project holds vast and promising opportunities. Future endeavors could focus on fortifying the system's security posture through the incorporation of advanced encryption algorithms. Exploration of dynamic payload adjustment mechanisms and real-time steganography for live video streams could further enhance the system's utility in real-world applications.

REFERENCES

[1]. Zhang, Rui, et al. "A Survey of Multimedia Data Hiding Technology." IEEE Access, vol. 6, 2018, pp. 11813-11833.

[2]. Rehman, Abdul et al. "Hybrid Encryption for Secure Communication in Multimedia IoT Systems." IEEE Transactions on Multimedia, vol. 21, no. 8, 2019, pp. 2070-2082.

[3]. Li, Xiang, et al. "Enhancing the Security of AES Algorithm through Hybrid Cryptography." International Journal of Computer Applications, vol. 177, no. 34, 2020, pp. 27-32.

[4]. Yang, Fan et al. "A New Video Steganography Method Based on LSB Matching and AES Encryption." Journal of Visual Communication and Image Representation, vol. 69, 2020, pp. 102824.

[5]. Yang, Yun, et al. "A Hybrid Video Steganography Algorithm Based on DWT and Chaos." IEEE Access, vol. 7, 2019, pp. 129509-129519

[6]. Jain, Nidhi, and Anand Sharma. "Secure Multimedia Communication Through Hybrid Cryptography and Steganography." International Journal of Computer Applications, vol. 179, no. 24, 2018, pp. 42-46.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303058 |

[7]. Zhang, Jun, et al. "A New Approach to Hybrid Image Steganography Using LSB and Cryptography." Multimedia Tools and Applications, vol. 79, no. 23-24, 2020, pp. 16385-16404.

[8]. Wang, Xin, et al. "A Secure and Robust Video Steganography Method Based on Hybrid Encryption." IEEE Access, vol. 9, 2021, pp. 137-146

[9]. Alghamdi, Abdullah, et al. "A Secure Data Hiding Technique Using Hybrid Cryptography." IEEE Access, vol. 8, 2020, pp. 33491-33504.

[10]. Gupta, Priya, et al. "Enhancing Data Security in Video Steganography using Hybrid Encryption Techniques." International Journal of Computer Science and Mobile Computing, vol. 8, no. 12, 2019, pp. 180-185.

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