IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

Multimedia Security through Video Steganography Using Hybrid Encryption

Harish Kumar P[1], Jisshnu H J[2], Deva M[3], Indumathi A[4]

U.G. Student, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India[1,2,3]

Associate Professor, Dept. of I.T., Sri Venkateswara College of Engineering, Sriperumbudur, Tamil Nadu, India[4]

ABSTRACT: In the digital age, safeguarding multimedia content is crucial, particularly during the transmission of sensitive data. This project presents an innovative solution to multimedia security by utilizing video steganography coupled with hybrid encryption. The main objective is to conceal multiple multimedia files within a video, ensuring their confidentiality and integrity during transmission. The methodology commences with the encryption of multimedia files using the robust Advanced Encryption Standard (AES) algorithm with a symmetric AES key. Subsequently, the AES key is encrypted using the RSA public key cryptography scheme. Afterwards, the encrypted AES key is subtly embedded into the video file utilizing sophisticated Least Significant Bit (LSB) steganography techniques, guaranteeing its invisibility to human perception. This hybrid encryption and steganography method offers a strong means of securely embedding multimedia files within a video, facilitating covert transmission and storage. The encryption protocol ensures that the hidden files maintain their confidentiality, while the steganography effectively conceals the presence of the concealed data. This inventive approach addresses the urgent requirement for multimedia security in scenarios where discreet transmission of sensitive information is necessary. It provides a reliable technique for preserving the confidentiality and integrity of multimedia files within a video format. By combining the strengths of encryption and steganography, this method establishes a robust defence against unauthorized access, providing assurance in the domain of multimedia data protection.

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

I. INTRODUCTION

In today's digitally interconnected world, the transmission of multimedia content poses a constant challenge in maintaining robust security and preserving confidentiality, particularly for sensitive information. While traditional encryption methods offer strong defences, they often falter when tasked with safeguarding the intricate fabric of multimedia files traversing networks. This challenge is exacerbated by the demand for covert transmission, where advanced security measures are imperative to maintain secrecy. Consequently, there arises an urgent need for a sophisticated and resilient approach to multimedia security—one that adeptly conceals multiple files within the layers of a video format, ensuring cryptic confidentiality, unwavering integrity, and virtually undetectable presence.

This project embarks on a journey to address this pressing challenge by pioneering a groundbreaking hybrid encryption and video steganography technique. This approach not only aims to establish 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.

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 lies 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.

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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

II. RELATED WORK

In [1] authors meticulously conduct a thorough literature review to investigate various steganography techniques, recognizing the limitations of traditional security measures in protecting sensitive data in today's digital environment. Their study encompasses a comprehensive analysis of existing cover steganography methods, evaluating their effectiveness, constraints, and potential improvements. By systematically categorizing and comparing methodologies across spatial space, transform domain, and adaptive space, the authors provide valuable insights into the intricacies of information hiding and detection. In [2] authors present an innovative approach to data security enhancement through steganography. By focusing on concealing information within 3D objects, the authors introduce a novel technique that combines Gray-code sequences with the Least Significant Bit (LSB) method to embed data securely within the vertex components of these objects. Their methodology is supported by a rigorous evaluation, which employs metrics such as Mean Square Error Ratio, Peak Signal-to-Noise Ratio, Histogram, and Normalized Correlation, demonstrating superior security levels compared to existing techniques. In [3] authors have introduced two new algorithms tailored for compressed videos encoded using the advanced H.264/AVC video coding standard. The first algorithm presents a robust video encryption technique based on chaotic maps with random keys. This approach aims to encrypt video data effectively, enhancing its resilience against various attacks while ensuring secure transmission and storage. The second algorithm combines steganography and cryptography, utilizing chaotic maps to embed and encrypt messages within video frames. By integrating these techniques, the authors aim to bolster the security of video content, shielding it from unauthorized access. In [4] authors introduce a groundbreaking data hiding algorithm tailored for 24-bit colour images. The primary objective is to address the escalating demand for steganography techniques capable of achieving remarkably high embedding capacities while preserving acceptable image quality, as measured by the peak signal-to-noise ratio (PSNR). Acknowledging the critical need for efficient data transmission, particularly in socially interactive and information-rich environments, the authors present the "spatial-domain-adjacent mean" algorithm. This novel approach enables the direct embedding of data into the spatial domain of images without necessitating complex transformations or training data, resulting in a significant augmentation of embedding capacity while mitigating fidelity loss. In [5] authors target digital video as a primary focus for their research due to its substantial capacity for data concealment. Identifying shortcomings in existing video steganography techniques, ranging from visual imperceptibility to embedding capacity, the authors propose a novel approach grounded in the principles of the Shi-Tomasi corner detector and the Least Significant Bits (LSBs) algorithm. Their methodology involves a multi-step process meticulously designed to ensure both security and imperceptibility. Initially, the Shi-Tomasi algorithm is utilized to identify regions within video frames characterized by corner points, chosen for their resilience against visual distortion. These areas serve as ideal candidates for data embedding. Subsequently, the 4-LSBs algorithm is employed to conceal confidential data within these corner points, leveraging their robustness and potential for high embedding capacity.

III. PROPOSED ALGORITHM

A. 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, $bit_{message}$)

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.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

DISADVANTAGES

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

B. SYSTEM ARCHITECTURE

OVERVIEW

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

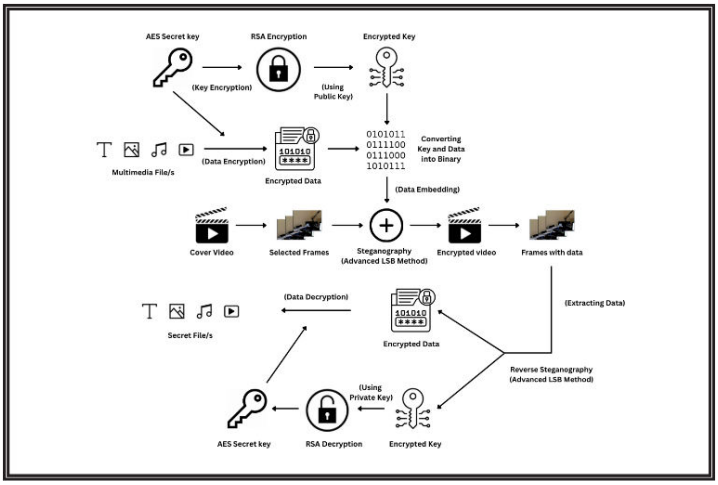

Fig.1 Architecture Diagram

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}).

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

AES ENCRYPTION

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

FORMULA

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

C. 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

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

D. 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.

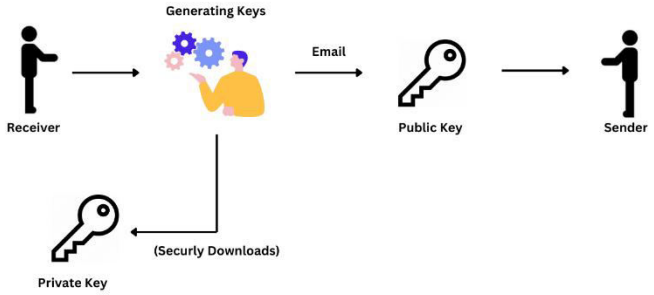

Fig.2 Key Generation

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.

E. STEGANOGRAPHY

OVERVIEW

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

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

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

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

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

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

I. 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

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

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

IV. RESULTS

The project aimed to assess the impact on video size after embedding data using hybrid encryption, balancing minimal distortion with security. Results showed a maximum increase in video size ranging from 40% to 70% of the original, consistently scalable across various multimedia file sizes and types. Visual inspection and perceptual testing confirmed the imperceptibility of the embedded data. Extensive testing evaluated the system's ability to securely hide and retrieve data, revealing successful concealment using AES encryption with a hybrid RSA key and seamless extraction procedures without loss or corruption. Additionally, steganographic video files exhibited seamless playback with no visible artifacts.

Tests on the system's robustness against steganalysis and decryption attempts showed resilience against steganalysis techniques, verified integrity through checksum verification of embedded files, and thwarted decryption attempts using unauthorized keys or methods, validating its security. Performance evaluation highlighted efficient processing speed, with operations completed within acceptable time frames, and CPU and memory usage within acceptable limits, indicating scalability. Overall, the system met objectives, providing a reliable method for secure data embedding. The user interface facilitated multimedia embedding and extraction using the hybrid encryption system, with user testing confirming ease of use and an intuitive design, enabling users to select files, configure encryption, and extract hidden data seamlessly. Positive user feedback emphasized the system's effectiveness in covertly transmitting sensitive multimedia.

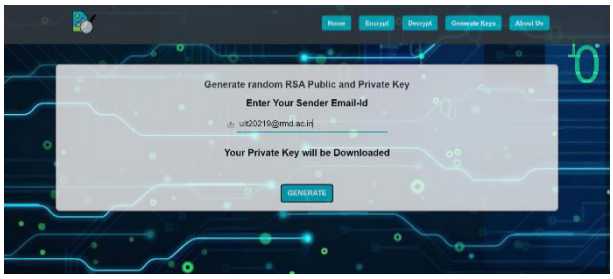

Fig.3 Generating RSA Keys

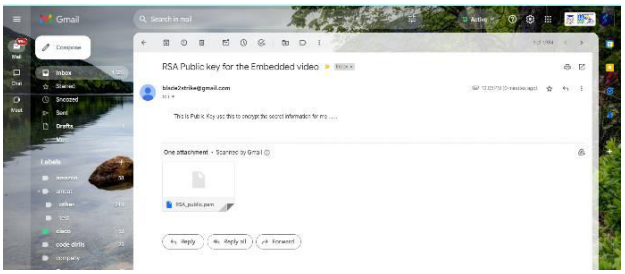

Fig.4 Public Key received in email

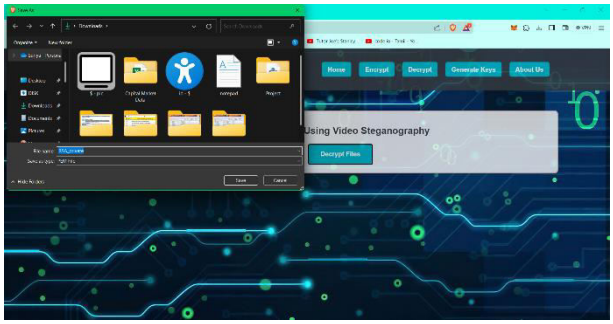

Fig.5 Downloading Private key

Fig.6 Encoding Files into video

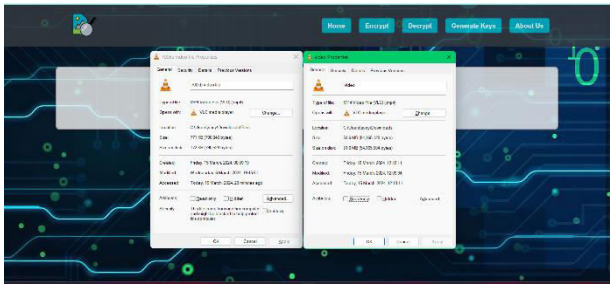

Fig.7 Video Before and After Embedding data

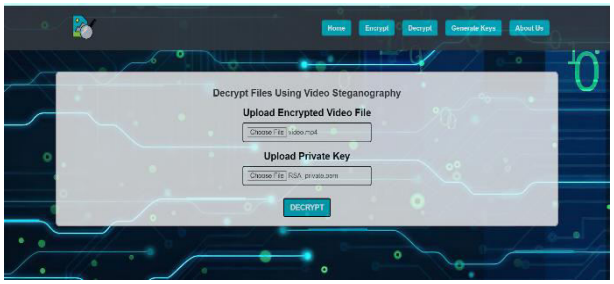

Fig.8 Decoding Files from video

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203110 |

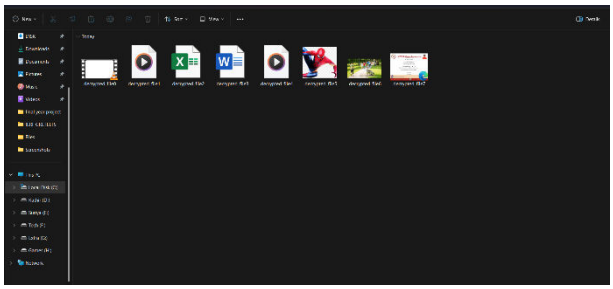

Fig.9 Decoded Files

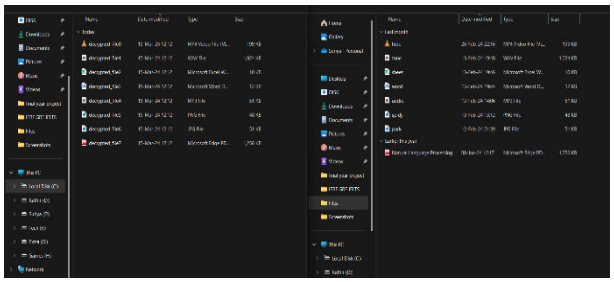

Fig.10 Original Files vs Decoded Files

V. CONCLUSION AND FUTURE WORK

In the realm of secure data communication and discreet information exchange, the fusion of multimedia video steganography with hybrid encryption emerges as a powerful solution. This project navigated through the complexities of concealing sensitive data within video streams while fortifying its security with hybrid encryption techniques. The primary goal of this endeavor was to develop an efficient and secure system capable of seamlessly embedding confidential information within video files, shielding it from unauthorized access and detection. By combining the strengths of symmetric and asymmetric encryption with the stealthiness of video steganography, we aimed to create a versatile tool for covert data transmission. Through an extensive review of existing literature, we explored multimedia steganography, video embedding methodologies, and the diverse landscape of encryption algorithms. Building upon this knowledge, we proposed a novel methodology that seamlessly integrates hybrid encryption with video steganography, ensuring both imperceptibility and data integrity. The implementation phase provided valuable insights into the practical challenges and intricacies of our proposed system. Leveraging cutting-edge tools and technologies, we demonstrated the feasibility and effectiveness of our approach. The experimental results, supported by comprehensive datasets and evaluation metrics, highlighted the system's ability to conceal significant volumes of data within video streams while preserving visual fidelity. Looking ahead, numerous promising opportunities await this project. Future endeavors could concentrate on enhancing the system's security posture through the adoption of advanced encryption algorithms. Exploring dynamic payload adjustment mechanisms and real-time steganography for live video streams could further augment the system's usability in real-world scenarios.

REFERENCES

1. Liu, Jia et al. "A Novel Approach to Video Steganography Based on Vector Quantization." Journal of Computer Science and Technology, vol. 26, no. 5, 2011, pp. 821-828.
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. Zhang, Rui, et al. "A Survey of Multimedia Data Hiding Technology." IEEE Access, vol. 6, 2018, pp. 11813-11833.
4. Fridrich, Jessica. "Steganography in digital media: Principles, algorithms, and applications." Cambridge University Press, 2009.
5. Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31.2 (1998): 26-34.
6. Stallings, William. "Cryptography and network security: Principles and practice." Pearson Education India, 2008.
7. Rijmen, Vincent, and Joan Daemen. "The design of Rijndael: AES-the advanced encryption standard." Springer, 2002.
8. Shamir, Adi, and Eran Tromer. "Steganography in silicon: hiding data in integrated circuits." IEEE Security & Privacy 4.4 (2006): 28-34.
9. 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.
10. 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details