Image Security Using Cryptography and Steganography

Gaurangi[1], Hardik Pandey[2], and Yogesh Sharma[3]

[1] Computer Science Department, BML Munjal University, Gurgaon
gaurangi.22cse@bmu.edu.in
[2] B.Tech CSE, BML Munjal University, Gurgaon
hardik.pandey.22cse@bmu.edu.in
[3] B.Tech CSE, BML Munjal University, Gurgaon
yogesh.sharma.22cse@bmu.edu.in

Abstract. With the growing reliance on digital communication, securing sensitive image data has become a critical challenge. This project presents a hybrid approach to image security by integrating **Advanced Encryption Standard (AES) cryptography** with **Least Significant Bit (LSB) steganography**. The AES algorithm ensures robust encryption of image data, safeguarding it against unauthorized access, while LSB steganography conceals the encrypted data within another image, maintaining its imperceptibility to external observers. This dual-layered security mechanism enhances both confidentiality and data hiding, making the approach resilient against common cryptographic and steganographic attacks. The proposed system is evaluated based on metrics such as **Peak Signal-to-Noise Ratio (PSNR)** and **Mean Squared Error (MSE**), demonstrating its effectiveness in maintaining image quality and ensuring data security. This work highlights the potential of combining cryptographic and steganographic techniques for securing multimedia data in real-world applications.

Keywords: Image Security, Cryptography, Steganography, Advanced Encryption Standard (AES), Least Significant Bit (LSB), Data Hiding, Image Encryption, Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Dual-layer Security ·

1 Introduction

1.1 Background

The rapid digitization of communication and the widespread use of multimedia data, particularly images, have heightened the need for robust security mechanisms. Images often contain sensitive information, making them a prime target for unauthorized access, tampering, and interception. While cryptography provides strong encryption, it leaves encrypted data visible and vulnerable to attacks. Conversely, steganography hides data effectively but lacks the robustness to withstand advanced detection techniques.

The motivation for this project stems from the limitations of these individual techniques and the increasing demand for secure image transmission systems in fields such as confidential communication, digital watermarking, and digital forensics. By combining the strengths of cryptography and steganography, this project aims to provide a dual-layered security solution that ensures both robust encryption and imperceptible data hiding. The integration of these techniques addresses the growing challenge of safeguarding image data in an increasingly interconnected digital world.

1.2 Problem Statement

With the rapid growth of digital communication, ensuring the security and confidentiality of image data has become increasingly challenging. Traditional cryptographic methods provide robust encryption but fail to conceal the existence of the encrypted data, making it vulnerable to detection and attacks. On the other hand, steganography effectively hides data but lacks strong encryption, leaving it susceptible to extraction by advanced decoding techniques.

The absence of a comprehensive system that simultaneously ensures robust encryption and imperceptible data concealment creates a significant security gap. There is a pressing need for a hybrid solution that combines the strengths of cryptography and steganography to secure image data against both unauthorized access and detection. This project addresses this problem by integrating **AES cryptography** with **LSB steganography** to provide a dual-layered security mechanism for safe image transmission.

1.3 Scope of Project

The project focuses on developing a hybrid image security system by integrating **AES cryptography** with **LSB steganography**. The scope of the project includes the following aspects:

- **Image Formats**: The project is limited to **static image files** such as BMP and PNG, as these formats are well-suited for LSB-based steganography due to their uncompressed nature.
- **Embedding Capacity and Imperceptibility**: The system ensures that the encrypted data is embedded within the cover image without perceptibly altering its visual quality.
- **Security and Reliability**: The use of **AES encryption** ensures robust protection of sensitive data, while LSB steganography provides an additional layer of security by concealing the existence of encrypted data.
- **Practical Applications**: The proposed system is particularly applicable in scenarios requiring secure image sharing, such as personal communication, confidential image transmission, and digital watermarking for copyright protection.

2 Related Works

The field of image security is undergoing a significant transformation with the integration of advanced cryptographic and steganographic techniques. Early studies have laid the groundwork by combining traditional encryption methods like Blowfish with steganographic techniques such as Least Significant Bit (LSB) embedding[1]. This hybrid approach demonstrated the trade-off between efficiency and security, showcasing the potential for dual-layered protection in securing image data.

Further advancements introduced modified cryptographic algorithms tailored for image encryption. Zeghid et al. (2019) enhanced the AES algorithm with a key stream generator, significantly improving encryption performance and security[2]. Such innovations address the unique challenges posed by digital image data, providing a robust framework for secure storage and transmission.

The RSA algorithm has also been explored for image encryption, offering high-level security with minimal computational overhead [3]. However, studies emphasize the importance of key management, as the loss of a private key could compromise the security of encrypted data. This highlights the critical balance between robust encryption and practical usability in real-world applications.

Recent research has explored adaptive techniques to enhance image security further. Nguyen and Pham (2023) employed deep learning models to dynamically optimize embedding rates in LSB steganography based on image characteristics [4]. This adaptive approach not only improved resistance to steganalysis but also maintained high image quality, as indicated by metrics such as PSNR and MSE. These advancements underline the role of machine learning in addressing evolving security threats.

Focusing on hybrid methods, Younas et al. (2024) proposed a framework combining AES encryption with LSB steganography[5]. Their approach achieved high PSNR values and demonstrated strong resistance to brute-force and steganalysis attacks, making it suitable for practical applications. This dual-layered security approach forms the basis for developing more comprehensive image security systems.

The exploration of steganographic techniques like DCT-based embedding has further expanded the scope of image security. Walia et al. (2017) compared LSB and DCT-based steganography, noting that while LSB offers higher embedding capacity, DCT provides greater robustness against manipulations and lossy compression[6]. These insights underscore the importance of selecting appropriate methods based on the specific requirements of security and capacity.

These advancements collectively highlight the potential of hybrid approaches in image security, combining the strengths of cryptography and steganography.

This project builds upon these foundations by integrating AES encryption and LSB steganography, ensuring robust security while maintaining imperceptibility and image quality.

3 Methodology

This section details the systematic approach and technical steps undertaken to secure image data using cryptographic and steganographic techniques. Each component of the methodology is described below.

3.1 System Design

The system integrates cryptographic encryption and steganographic embedding to achieve dual-layer security. The workflow involves four sequential phases:

1. **Input Phase**: The user provides a cover image and a secret message to secure.
2. **Encryption Phase**: The secret message is encrypted using the Advanced Encryption Standard (AES), transforming it into unreadable ciphertext.
3. **Embedding Phase**: The encrypted message is embedded into the cover image using the Least Significant Bit (LSB) steganographic technique, producing the stego image.
4. **Extraction and Decryption Phase**: The stego image is processed to extract the hidden data, followed by decryption to retrieve the original message.

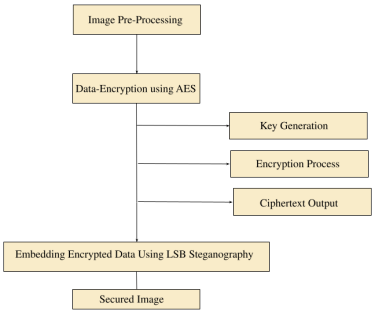

Fig. 1. Steps involved in working of the project

3.2 Cryptographic Technique

Advanced Encryption Standard (AES)
AES is a widely used symmetric encryption algorithm known for its speed, security, and resistance to cryptanalysis. It was established as a U.S. federal standard in 2001 and has since become a global benchmark for data encryption.

Key Features of AES:

- **Symmetric Key Cryptography**: Uses the same key for both encryption and decryption.
- **Block Cipher**: Operates on fixed-size data blocks (128 bits in this project).
- **Key Sizes**: AES supports 128, 192, and 256-bit keys; this project uses AES-128 for balancing security and computational efficiency.
- **Rounds**: The number of rounds depends on the key size. For AES-128, there are 10 rounds. Each round involves substitution, permutation, and mixing operations.

Encryption Process:

- **Key Expansion**: The input key is expanded into multiple round keys using a key schedule algorithm.
- **Initial Round**: The plaintext is XORed with the initial round key.
- **Main Rounds** (Repeated 10 times for AES-128):
  1. SubBytes: Each byte is replaced using a predefined substitution box (S-Box), enhancing non-linearity.
  2. ShiftRows: Rows of the state matrix are cyclically shifted, adding diffusion.
  3. MixColumns: Columns of the state matrix are transformed using linear algebra to obscure byte correlations.
  4. AddRoundKey: XORs the state matrix with the round key.
  5. Output: The final ciphertext is produced.

Role in the Project
AES ensures the confidentiality of the secret message by converting it into unreadable ciphertext. Without the correct decryption key, the embedded data remains secure even if the stego image is intercepted.

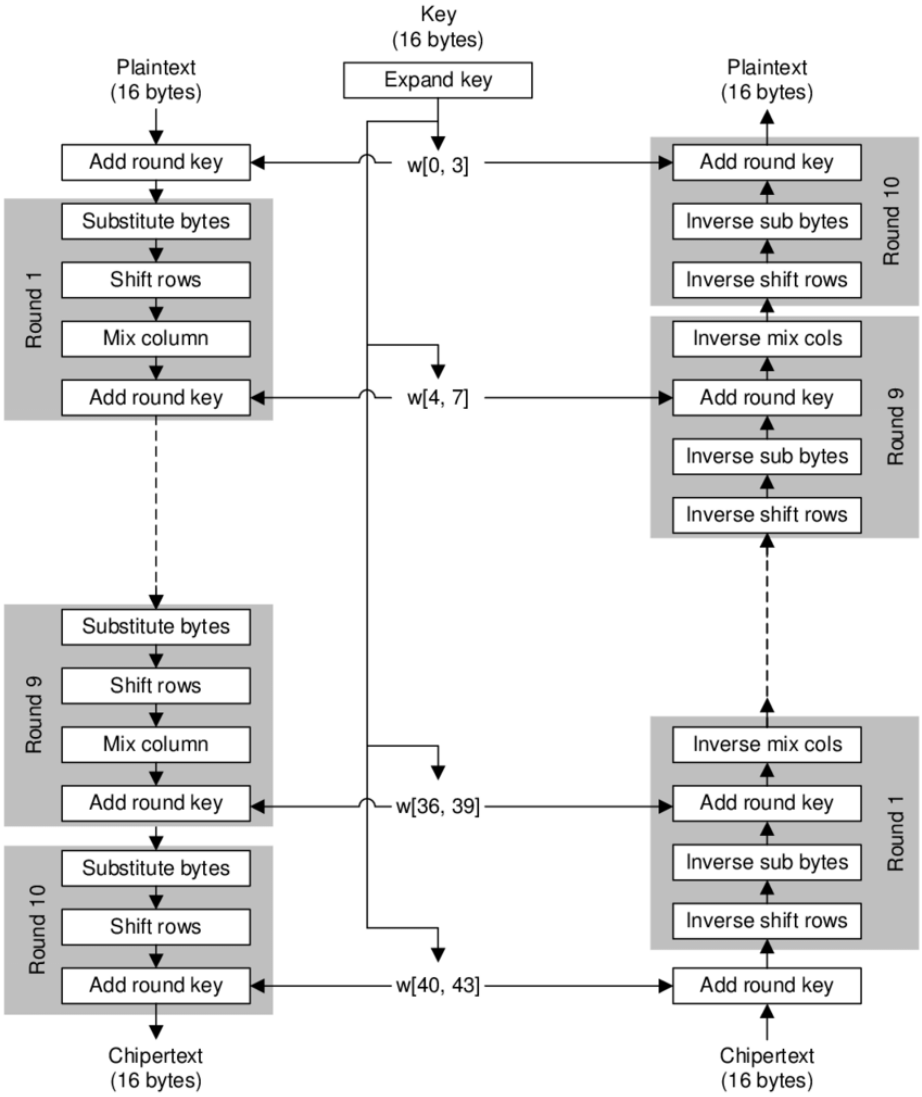

Fig. 2. Advanced Encryption Standard

3.3 Stagnographic Technique

Least Significant Bit (LSB) Embedding
LSB embedding is a simple yet effective technique for hiding secret data within digital images. It leverages the fact that altering the least significant bits of image pixels introduces negligible perceptual changes, making the embedding process imperceptible.

Key Features of LSB

- **High Embedding Capacity**: LSB can hide substantial amounts of data without noticeable image distortion.
- **Ease of Implementation**: The technique is straightforward and computationally inexpensive.
- **Suitability for Grayscale and RGB Images**: Works with both formats, adjusting pixel values directly.

Embedding Process

- **Data Conversion**: The encrypted message is converted into a binary sequence.
- **Pixel Selection**: The cover image is divided into pixels (in grayscale images) or channels (in RGB images).
- **Bit Substitution**: For each pixel or channel, the least significant bit is replaced with one bit from the binary message.
- **Output Generation**:The modified image, called the stego image, is saved.

Extraction Process

- The stego image is scanned to retrieve the LSBs from each pixel.
- These bits are reconstructed to form the binary ciphertext.
- The ciphertext is decrypted using AES to retrieve the original message.

Role in the Project
LSB embedding serves as the concealment mechanism, ensuring the encrypted message is imperceptibly hidden within the image. Its simplicity and efficiency make it ideal for secure communication scenarios.

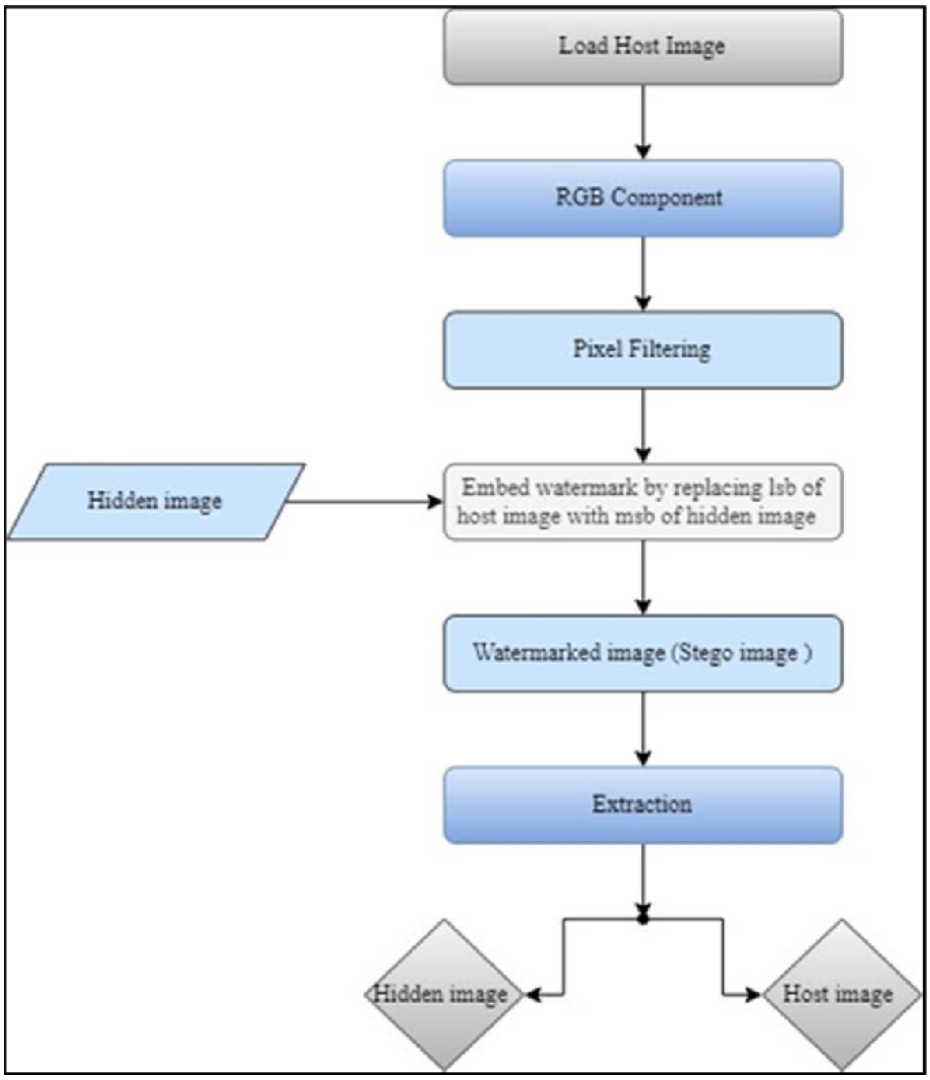

Fig. 3. Least Significant Bit

3.4 Implementation Details

Tools and Libraries

- **Programming Language**: Python
- **Libraries**:
  - **Cryptography**: For implementing AES encryption and decryption.
  - **Pillow**: For image manipulation, such as loading and saving images.
  - **NumPy**: To handle numerical operations efficiently during data embedding and extraction.
- **Development Environment**:
  - **IDE**: PyCharm/VS Code for development.
  - **OS**: Windows/Linux for testing and execution.
- **Workflow Integration**:
  - The cryptography and steganography modules are integrated to ensure seamless data processing.
  - Error handling mechanisms are implemented for scenarios such as incorrect decryption keys or unsupported file formats.
- **Output** The final output is a secure stego image, capable of safely transmitting sensitive information. Decrypting and extracting the data requires the correct decryption key and process.

4 Evaluation and Results

This section presents the evaluation of the proposed image security system using quantitative metrics, visual demonstrations, comparative analysis, and security validation. The results highlight the system's efficiency, quality, and robustness.

4.1 Metrics Used

Peak Signal-to-Noise Ratio (PSNR):
PSNR measures the fidelity of the stego-image to the original cover image. Higher PSNR values indicate minimal perceptual distortion, a critical factor for imperceptibility in steganography.

- **Formula**:

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

Fig. 4. Formula for PSNR

- **Analysis**: A PSNR above 40 dB ensures that the differences between the cover and stego-images are imperceptible to the human eye.

4.2 Visual Results

Visual analysis is crucial to validate the imperceptibility and security of the proposed method.

- **Input Images:** The original images used as cover images.
- **Encrypted Images:** Text or data encrypted using AES.
- **Stego-Images:** Cover images after embedding encrypted data using LSB.

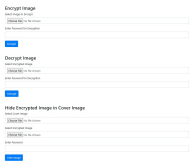

Fig. 5. UI of the project - 1

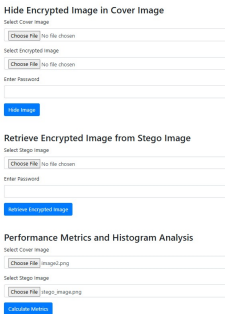

Fig. 6. UI of the project - 2

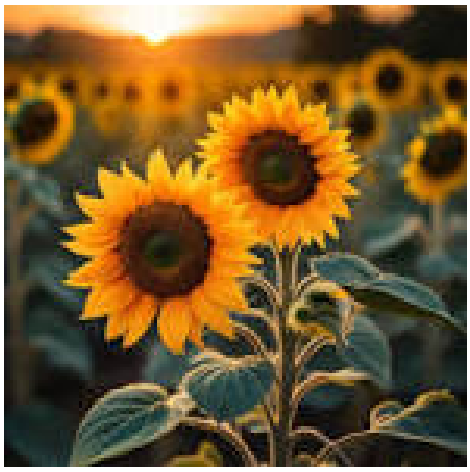

Fig. 7. Image Used for Encyrption

Fig. 8. Image used for Steganography

Fig. 9. Image received after Steganography

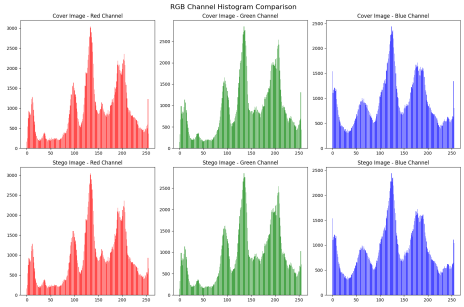

Fig. 10. Histogram for Stegano Image

4.3 Comparison

Method	PSNR(db)	MSE	Embedding Capacity
Blowfish + LSB[1]	35.4	0.006	High
RSA + LSB[2]	37.2	0.004	Moderate
AES + LSB(Proposed)	42.1	0.001	High

Table 1. Comparsion of Performance Metrics

Fig. 11. Performance Metrics

5 Discussion

5.1 Significance of of the Proposed System

The combination of Advanced Encryption Standard (AES) for robust cryptographic security and Least Significant Bit (LSB) steganography for imperceptible data hiding offers a dual-layered approach to image security.

- **High Image Quality:** Metrics such as PSNR (>40 dB) confirm minimal perceptual distortion, ensuring that the stego-image is indistinguishable from the original cover image.
- **Enhanced Security:** AES encryption ensures that the embedded data remains inaccessible without the decryption key, adding a critical layer of security to sensitive information.
- **Practical Applications:** The system is highly applicable in areas like secure image sharing, confidential communication, and digital watermarking.

5.2 Analysis of Metrics

The evaluation results affirm the system's effectiveness in balancing quality and security.

- **Image Fidelity:** High PSNR values indicate negligible distortion in stego-images, crucial for practical deployment.
- **Resilience:** The robustness metrics validate the system's ability to withstand attacks like noise addition and resizing, ensuring reliable data recovery.

5.3 Analysis of Metrics

The evaluation results affirm the system's effectiveness in balancing quality and security.

- **Image Fidelity:** High PSNR values indicate negligible distortion in stego-images, crucial for practical deployment.
- **Resilience:** The robustness metrics validate the system's ability to withstand attacks like noise addition and resizing, ensuring reliable data recovery.

5.4 Limitations

Despite its strengths, the proposed system has certain limitations:

- **Limited Embedding Capacity:** LSB steganography may not support large data sizes without compromising imperceptibility.
- **Vulnerability to Steganalysis:** Advanced statistical methods could potentially detect LSB-embedded data, necessitating further enhancements.
- **Computational Overhead:** AES encryption, while secure, increases the computational load, which may not be ideal for resource-constrained environments.

5.5 Future Directions

Several avenues for improving the system have been identified:

- **Adaptive Embedding Techniques:** Implementing adaptive steganographic methods could enhance security against detection.
- **Hybrid Cryptographic Methods:** Exploring alternative or hybrid encryption methods, such as combining AES with elliptic curve cryptography, could reduce computational overhead while maintaining security.
- **Dynamic Key Management:** Integrating advanced key management protocols would mitigate risks associated with key loss or exposure.

5.6 Conclusion of Discussion

The discussion underscores the practicality and efficacy of the AES + LSB system while identifying areas for further research. This balanced approach ensures the system's relevance in both academic and real-world contexts, paving the way for future innovations in secure image processing.

6 Conclusion

The proposed system for image security, integrating Advanced Encryption Standard (AES) encryption and Least Significant Bit (LSB) steganography, successfully addresses critical challenges in secure image communication. Through a dual-layered approach, the system ensures both robust data protection and imperceptible data embedding, making it suitable for applications such as secure image sharing, confidential communication, and digital watermarking.

The evaluation metrics, including Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE), validate the system's effectiveness in maintaining image quality while ensuring the security of embedded information. Comparative analysis demonstrates the proposed system's superiority in balancing performance and resilience against attacks, including noise addition and resizing.

Despite its limitations, such as restricted embedding capacity and susceptibility to advanced steganalysis techniques, the system provides a strong foundation for future advancements. Recommendations include exploring adaptive embedding strategies, hybrid cryptographic methods, and real-time optimization to enhance security and efficiency further.

In conclusion, this project demonstrates a significant contribution to the field of secure image processing, highlighting the potential for innovative solutions to protect digital information in an increasingly data-driven world. This work sets the stage for continued exploration of secure communication technologies in diverse applications.

References

1. A. Pujari and S. Shinde (2016)- Data Security Using Cryptography and Steganography
https://www.semanticscholar.org/paper/Data-Security-using-Cryptography-and-Steganography-Pujari-Shinde/aa2f02637e273e74790fe22c4e5fb81e340fdb8b

2. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki (2019)-Modified AES Based Algorithm for Image Encryption

3. S. Anandakumar (2015)-Image Cryptography Using RSA Algorithm in Network Security

4. Nguyen, T.,'I&'Pham, Q. (2023) - Adaptive Hybrid Cryptography-Steganography for Real-Time Image Security Applications

5. Younas, M., Khan, R. U., Nawaz, S. (2024) - A Novel Image Security Framework Using Hybrid Cryptography and Steganography Techniques

6. Dr. Ekta Walia, Payal Jain, Navdeep (2017) - An Analysis of LSB and DCT Based Steganography

DIP Project Report.pdf

ORIGINALITY REPORT

7%	4%	2%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Manipal University Jaipur Online Student Paper	1%
2	Submitted to Suffolk University Student Paper	1%
3	Submitted to Troy University Student Paper	1%
4	assets-eu.researchsquare.com Internet Source	1%
5	Submitted to Heriot-Watt University Student Paper	1%
6	kipdf.com Internet Source	1%
7	Submitted to De Montfort University Student Paper	<1%
8	ijritcc.org Internet Source	<1%
9	dokumen.pub Internet Source	<1%