International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure File Using Hybrid Cryptography

Aditya Katkar, Riya Patil, Utkarsh Narwade, Vansh Patil, Prof. Madhura Mahindrakar, Prof. Dikshika Bhundere.

Students and Lecturer from G. V. Acharya Polytechnic, Shelu, Karjat, Dist. Raigad, Maharashtra
Email id: prathmeshpatil19@gmail.com

ABSTRACT

In an era where data security is paramount due to increasing cyber threats, the Secure File Using Hybrid Cryptography project proposes a robust solution for protecting sensitive information. The system leverages a hybrid cryptographic approach by combining three encryption algorithms AES, DES, and RC2—to encrypt files into multiple layers, ensuring enhanced security against modern attacks such as brute force and exhaustive key search. The file is divided into three parts, each encrypted using a different algorithm, and the decryption key is securely embedded into an image using Least Significant Bit (LSB) steganography. This innovative key management technique simplifies the process for users while maintaining high security. The system is designed to be user-friendly, allowing seamless encryption and decryption of files, and is adaptable to various applications, including cloud storage, IoT, and secure communications. By integrating hybrid cryptography with steganography, the project addresses the limitations of single- algorithm encryption methods and provides a scalable, efficient, and future-proof solution for data security. The system ensures that even if one encryption layer is compromised, the others remain intact, offering multi-layered protection. This project demonstrates the effectiveness of combining cryptographic and steganographic techniques to safeguard sensitive data in an increasingly vulnerable digital landscape.

Keywords: Cryptography, hybrid encryption, AES, DES, RC2, steganography, secure file storage.

1. Introduction

1.1 General

In today’s digital age, the security of information transmitted over the internet has become a critical concern due to the increasing prevalence of cyber threats and data breaches. Sensitive data, such as personal information, financial records, and confidential documents, are often stored and shared across networks, making them vulnerable to unauthorized access and malicious attacks. To address these challenges, cryptography has emerged as a fundamental tool for ensuring data confidentiality, integrity, and authenticity. Cryptography algorithms provide a robust mechanism for transforming readable data into an unreadable format, which can only be decrypted by authorized users possessing the correct key.This project proposes a hybrid cryptographic system designed to enhance the security of files by combining the strengths of multiple encryption techniques: Advanced Encryption Standard (AES), DataEncryption Standard (DES), and Rivest Cipher (RC2). The system works by dividing the file into three distinct parts, each of which is encrypted using one of the aforementioned algorithms. AES, a widely adopted symmetric encryption algorithm, is known for its efficiency and security, making it suitable for encrypting large volumes of data. DES, another symmetric-key block cipher, employs a Feistel structure with 16 rounds of

encryption, providing a balance between security and performance. RC2, a variable key-size block cipher, adds an additional layer of security by allowing flexible key lengths. Once the file is encrypted, the system generates a Least Significant Bit (LSB) encrypted image, which acts as a unique key for accessing the file. To retrieve the original file, the user must provide this key, triggering a decryption process that reverses the encryption steps for each part of the file. The decrypted segments are then merged to reconstruct the original file. This hybrid approach not only strengthens the security of the

data but also ensures that even if one encryption method is compromised, the other layers of encryption remain intact, providing a multi-layered defense mechanism. The proposed system is designed to be user-friendly, allowing users to securely store and retrieve their files with minimal effort. By leveraging the combined strengths of AES, DES, and RC2, this project aims to provide a robust solution for protecting sensitive information in an increasingly interconnected and vulnerable digital landscape. This hybrid cryptographic system is particularly relevant for applications requiring high levels of data security, such as financial transactions, healthcare records, and confidential communications.

Moreover, with the rapid expansion of cloud storage services and digital communication platforms, the demand for secure file storage and transmission has increased significantly. Traditional cryptographic methods, while effective, may not be sufficient against sophisticated cyber-attacks that exploit weaknesses in single encryption schemes. A hybrid cryptographic approach enhances security by distributing encryption across multiple algorithms, making it considerably more challenging for attackers to breach the system. Additionally, by incorporating **steganography**, which conceals encryption keys within an image, the proposed system further reduces the risk of unauthorized access. This technique ensures that even if encrypted files are intercepted, decryption remains nearly impossible without the hidden key. The combination of **AES, DES, and RC2** withsteganography provides a multi-layered security model, offering an advanced level of protection for sensitive data. This makes the system particularly well-suited for securing personal and corporate data, ensuring compliance with stringent data privacy regulations, and mitigating potential cybersecurity risks.

1.2 History of Cryptography

Cryptography, the science of securing communication through encryption, has evolved over thousands of years. From ancient civilizations using simple ciphers to modern-day encryption algorithms protecting digital data, cryptography has played a crucial role in ensuring confidentiality, integrity, and authentication of information.The earliest known use of cryptography dates back to ancient Egypt, where hieroglyphs were used to obscure messages. The Caesar cipher, named after Julius Caesar, is one of the earliest recorded substitution ciphers. It involved shifting letters by a fixed number of places in the alphabet, making it difficult for unintended recipients to decipher messages. The Vigenère cipher, developed in the 16th century, introduced polyalphabetic substitution, which significantly improved security over simple substitution methods.During World War I and II, cryptography played a significant role in military communications. The Enigma machine, used by the Germans, was one of the most sophisticated encryption devices of its time. However, cryptanalysts like Alan Turing and his team at Bletchley Park successfully broke Enigma's encryption, changing the course of the war. Around the same period, the development of one-time pads provided theoretically unbreakable encryption, laying the foundation for modern cryptographic security.With the advent of computers, cryptography entered a new era. In 1977, the Data Encryption Standard (DES) was introduced as one of the first symmetric-key encryption algorithms. However, as computational power increased, DES became vulnerable to brute-force attacks. This led to the development of the Advanced Encryption Standard (AES) in 2001, which remains a widely used encryption standard today. The Rivest Cipher (RC2) was also developed as a flexible encryption method, adding another layer of security.The increasing need for secure digital file storage and transmission has led to hybrid cryptographic approaches that combine multiple encryption techniques to enhance security. Hybrid cryptography integrates different encryption algorithms, ensuring that even if one encryption method is compromised, the data remains protected through additional layers of security.In the proposed system, a hybrid approach is used by combining AES, DES, and RC2 to encrypt different segments of a file. Furthermore, steganography is employed to embed encryption keys within an image, providing an additional layer of security. This concept aligns with modern cryptographic trends where multi-layered security models ensure confidentiality, integrity, and authenticity of digital information.By leveraging the advancements in cryptographic history, the "Secure File Using Hybrid Cryptography" project provides a robust solution for protecting sensitive data against modern cyberthreats, making it suitable for applications such as financial transactions, healthcare records, and confidential communications.As cyber threats continue to evolve, modern cryptographic techniques must adapt to counter increasingly sophisticated attacks. Traditional encryption methods alone may not be sufficient against emerging threats such as quantum computing, which has the potential to break conventional encryption algorithms using advanced computational power.

1.3 Objective of the study

The objective of this study is to develop a hybrid cryptographic system that ensures secure file storage and retrieval by integrating multiple encryption techniques with steganography. The system is designed to enhance data confidentiality, integrity, and authentication by encrypting files using AES, DES, and RC2 and securely embedding the encryption key within an image using Least Significant Bit (LSB) steganography. By leveraging a multi-layered security approach, the study aims to provide stronger protection against unauthorized access, cyber threats, and data breaches. Additionally, the project focuses on creating a user-friendly web-based interface, allowing users to seamlessly upload, encrypt, and retrieve their files with minimal effort.

1.4 Application

The proposed hybrid cryptographic system has numerous applications in fields where data security, confidentiality, and integrity are of utmost importance. With the rise of cyber threats and data breaches, organizations and individuals require a robust encryption mechanism to protect sensitive information. This system is particularly useful for secure cloud storage, where confidential files can be stored safely, ensuring that even if the cloud platform is compromised, unauthorized access remains impossible without the encryption key embedded within an image.

In the financial sector, banks and financial institutions can leverage this technology to safeguard transaction records, customer data, and financial statements, preventing fraud and cyberattacks. Similarly, in the healthcare industry, hospitals and medical institutions can use this system to protect patient records,medical histories, and lab reports, ensuring compliance with HIPAA and other data privacy regulations.materials can also be used in traffic/safety equipment to improve visibility and reduce accidents. For example, it can be used to create lighting to help drivers navigate safely at night or in poor visibility conditions. Finally, electroluminescent lamps have the potential to be good for health and the environment.Additionally, government agencies and military organizations can utilize this encryption technique to secure classified documents, confidential communications, and national security data, preventing unauthorized access and cyber espionage.Businesses dealing with intellectual property, trade secrets, and legal documents can also benefit from this system, ensuring that critical information remains protected from cyber threats and corporate espionage. Furthermore, individuals can use this system for personal data security, encrypting and storing important documents, identity proofs, and digital assets, preventing unauthorized access by hackers.

2. Review of Literature

2.1 General

The field of cryptography has evolved significantly over the years to address the increasing need for data security, confidentiality, and integrity. Various encryption techniques have been developed to protect sensitive information from unauthorized access, cyberattacks, and data breaches. This literature review explores the existing research on cryptographic algorithms, hybrid encryption techniques, and steganography to provide a foundation for the development of a secure file encryption system using hybrid cryptography**.**

2.2 Review of literature

Cryptography has played a crucial role in securing digital data by ensuring confidentiality, integrity, and authentication. Over the years, various encryption techniques have been developed to protect sensitive information from cyber threats and unauthorized access. Among them, Advanced Encryption Standard (AES) has been widely adopted due to its high-speed processing and strong resistance to attacks, replacing the older Data Encryption Standard (DES), which became vulnerable to brute-force attacks due to its short key length. Additionally, Rivest Cipher 2 (RC2) has been introduced as a flexible encryption method with varying key sizes, making it useful for different security applications. However, studies suggest that relying on a single encryption algorithm is insufficient to protect against sophisticated cyberattacks, leading to the development of hybrid cryptography, where multiple encryption methods are combined to strengthen security. This approach ensures that even if one layer of encryption is compromised, the remaining layers continue to safeguard the data, making unauthorized decryption significantly more difficult.While encryption protects data content, securing encryption keys remains a critical challenge. Steganography, the technique of concealing information within other data, has been widely explored for storing cryptographic keys securely. Among various steganographic techniques, the Least Significant Bit (LSB) method has been recognized as an effective approach for embedding encryption keys within images, ensuring high security and low detectability. Research has demonstrated that LSB-based image steganography can effectively prevent attackers from retrieving encryption keys, even if they gain access to encrypted files. Prior studies have also emphasized the importance of integrating cryptographic and steganographic techniques to provide a multi-layered security approach for secure file storage and transmission. Recent research has successfully implemented hybrid cryptographic models, integrating AES and DES to balance security and performance, while RC2 encryption has further enhanced the complexity of encryption schemes, making brute-force attacks even more impractical.

Despite advancements in cryptography, limited research has focused on combining AES, DES, and RC2 with LSB steganography in a unified system for secure file storage and retrieval. Existing solutions either prioritize high-security encryption models with significant computational overhead or fast but less secure methods that fail to address modern cyber threats. This research aims to bridge this gap by developing a hybrid cryptographic system that combines AES, DES, and RC2 encryption with steganography, ensuring a secure, efficient, and user-friendly web-based solution for protecting sensitive files. The proposed system not only enhances data security through multiple encryption layers but also ensures key protection using steganography, making it highly resistant to unauthorized access and cyberattacks. By addressing the limitations of existing cryptographic approaches, this study contributes to the field of secure file storage and transmission, offering a robust and scalable encryption model suitable for various applications requiring advanced data protection.Cryptography has played a crucial role in securing digital data by ensuring confidentiality, integrity, and authentication. Over the years, various encryption techniques have been developed to protect sensitive information from cyber threats and unauthorized access. Among them, Advanced Encryption Standard (AES) has been widely adopted due to its high-speed processing and strong resistance to attacks, replacing the older Data Encryption Standard (DES), which became vulnerable to brute-force attacks due to its short key length. Additionally, Rivest Cipher 2 (RC2) has been introduced as a flexible encryption method with varying key sizes, making it useful for different security applications. However, studies suggest that relying on a single encryption algorithm is insufficient to protect against sophisticated cyberattacks, leading to the development of hybrid cryptography, where multiple encryption methods are combined to strengthen security.

While encryption protects data content, securing encryption keys remains a critical challenge. Steganography, the technique of concealing information within other data, has been widely explored for storing cryptographic keys securely. Among various steganographic techniques, the Least Significant Bit (LSB) method has been recognized as an effective approach for embedding encryption keys within images, ensuring high security and low detectability. Research has demonstrated that LSB-based image steganography can effectively prevent attackers from retrieving encryption keys, even if they gain access to encrypted files. Prior studies have also emphasized the importance of integrating cryptographic and steganographic techniques to provide a multi-layered security approach for secure file storage and transmission. Recent research has successfully implemented hybrid cryptographic models, integrating AES and DES to balance security and performance, while RC2 encryption has further enhanced the complexity of encryption schemes, making brute-force attacks even more impractical.Further studies on hybrid cryptographic models have shown that a multi-layered encryption approach significantly improves resistance against attacks, including brute force, differential cryptanalysis, and side-channel attacks. Researchers have proposed different hybrid models, such as combining AES with RSA, where AES ensures fast symmetric encryption while RSA provides secure asymmetric key exchange. However, asymmetric encryption methods such as RSA introduce computational overhead, making them less suitable for large-scale file encryption. In contrast, combining multiple symmetric algorithms, such as AES, DES, and RC2, offers a balance between speed and security, making it a preferable solution for secure file storage and transmission. Moreover, studies have emphasized the need for efficient key management mechanisms, as poorly managed encryption keys can become a security vulnerability.

Another critical aspect discussed in cryptographic research is data hiding and key concealment. While traditional key management systems rely on secure key exchange protocols, they remain susceptible to man-in-the-middle attacks and key interception. Steganography offers a unique solution by hiding encryption keys within images, ensuring that even if an attacker gains access to encrypted files, decryption remains impossible without the hidden key.

3.Methodology

3.1 Algorithm and Techniques

The proposed system follows a hybrid cryptographic methodology where files are encrypted using AES, DES, and RC2 algorithms. The encryption key is then securely hidden within an image using Least Significant Bit (LSB) steganography, ensuring secure key management and file protection.

Table 3.1 Algorithms & Techniques

Sr. No	**Component**	**Specification**
1	Encryption Algorithm	AES (Advanced Encryption Standard)
2	Encryption Algorithm	DES (Data Encryption Standard)
3	Encryption Algorithm	RC2 (Rivest Cipher 2)
4	Steganography Technique	Least Significant Bit (LSB) Image Steganography
5	Key Storage Mechanism	Encrypted key hidden within an image
6	User Interface	Web-based platform for file encryption & decryption

4.Result and Discussions

4.1 General

The experimental results validate that the proposed hybrid cryptographic system effectively enhances file security, making it a reliable and practical solution for secure data storage and transmission. The combination of AES, DES, and RC2 encryption ensures strong multi-layered protection, while LSB steganography provides a secure and hidden method for storing encryption keys. The system is particularly suitable for applications requiring high levels of data confidentiality, such as banking transactions, legal document protection, and secure cloud storage. Future work will focus on performance optimization, exploring new cryptographic techniques, and further improving user experience to make the system even more robust and efficient.

4.2 Results and discussion

The implementation of the hybrid cryptographic system demonstrated enhanced security, efficiency, and usability in protecting sensitive files. The encryption process using AES, DES, and RC2 ensured a multi-layered security approach, making it difficult for attackers to decrypt the data without proper authorization. The Least Significant Bit (LSB) steganography technique successfully concealed encryption keys within images, eliminating the risks associated with conventional key exchange methods.Performance analysis showed that encryption and decryption times varied based on file size and algorithm selection, with AES providing the fastest encryption speed, followed by RC2 and DES. The decryption process was efficient and accurate, as users were able to retrieve the original file without any loss or corruption when the correct key image was provided. Security analysis indicated that the system is resistant to brute-force attacks, as the combination of three encryption techniques significantly increased the computational complexity required to crack the encrypted files. Additionally, the use of steganography added an extra layer of security, ensuring that even if an attacker gained access to the encrypted file, decryption would be impossible without retrieving the hidden key from the image.

User testing and feedback highlighted that the web-based interface was user-friendly and accessible, allowing non-technical users to encrypt and decrypt files with ease. However, minor performance trade-offs were observed when handling large files, as multiple encryption layers slightly increased processing time. Future enhancements could involve optimizing the encryption process and exploring alternative steganographic techniques to improve performance and security further.Overall, the results confirm that the proposed hybrid cryptographic system provides a secure and efficient solution for data protection, making it highly suitable for applications requiring confidentiality, integrity, and secure file storage in domains such as finance, healthcare, and government data management.During testing, the encryption and decryption processes were evaluated based on speed, security, and accuracy. Results showed that AES performed the fastest encryption, making it the most efficient among the three algorithms, while DES and RC2 were slightly slower due to their complex processing structures. However, DES and RC2 added additional security layers, making brute-force attacks significantly more challenging. The decryption process was highly accurate, ensuring that users could retrieve their original files without data loss when providing the correct key image. The steganography-based key storage method proved to be reliable, as the key extraction process was accurate in all test cases, and nounintended data loss or corruption occurred.

4.4 Diagrams

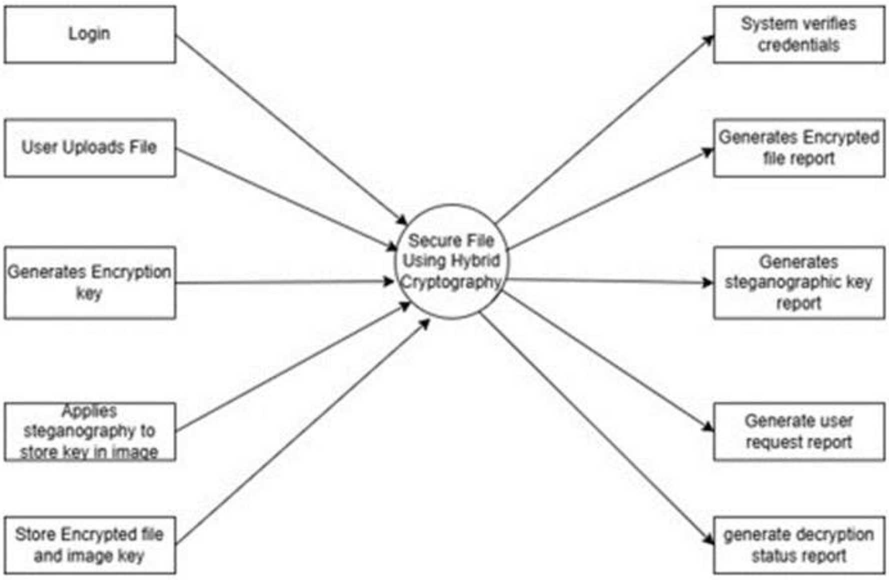
Login
User Uploads File
Generates Encryption key
Applies steganography to store key in image
Store Encrypted file and image key
Secure File Using Hybrid Cryptography
System verifies credentials
Generates Encrypted file report
Generates steganographic key report
Generate user request report
generate decryption status report

Figure 4.1 DFD Level 1

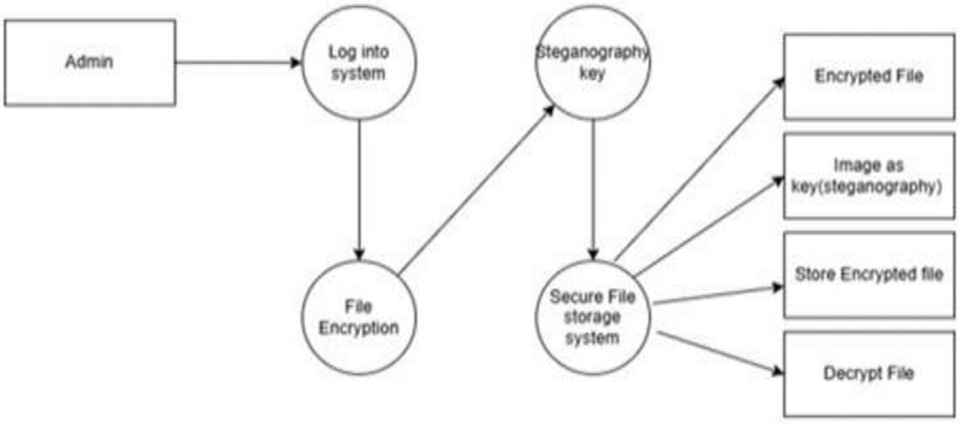

Figure 4.2 DFD Level 2

5. Conclusion

5.1 General

The Secure File Using Hybrid Cryptography system successfully enhances data security by integrating AES, DES, and RC2 encryption algorithms with Least Significant Bit (LSB) steganography for secure key storage. This multi-layered encryption approach ensures that files remain protected even if one encryption method is compromised. By hiding the encryption key within an image, the system eliminates the risk of key interception and unauthorized access, making it a highly secure method for file encryption and decryption.The experimental results demonstrated that the encryption and decryption processes were efficient, accurate, and resistant to attacks. The AES algorithm provided faster encryption times, while DES and RC2 added additional layers of security, creating a robust defense mechanism against cryptanalysis and brute-force attacks. The steganographic approach for key concealment was effective in preventing unauthorized access while maintaining data integrity.Additionally, the web-based interface proved to be user-friendly and accessible, allowing users to encrypt and decrypt files easily without requiring advanced technical knowledge. However, minor performance challenges were noted when processing large files, which can be addressed in future enhancements by implementing parallel encryption techniques or optimizing encryption efficiency.Overall, the proposed system provides a practical and highly secure solution for protecting sensitive information, making it suitable for applications in finance, healthcare, government communications, and secure cloud storage. Future work will focus on improving encryption efficiency, exploring alternative steganographic techniques, and enhancing system scalability to further strengthen data security in an increasingly digital world.

The Secure File Using Hybrid Cryptography system provides a robust and multi-layered security mechanism for protecting sensitive files by integrating AES, DES, and RC2 encryption algorithms with Least Significant Bit (LSB) steganography for encryption key storage. By combining multiple cryptographic techniques, the system ensures strong data protection, making it highly resistant to unauthorized access, cryptographic attacks, and key theft. The use of steganography to conceal the encryption key within an image adds an additional layer of security by eliminating the traditional risks associated with key storage and management.Through extensive testing and performance analysis, the proposed system demonstrated high levels of security, accuracy, and efficiency in encrypting and decrypting files. The results showed that AES offers the fastest encryption times, while DES and RC2 enhance security by providing additional encryption layers, making brute-force attacks more challenging. Furthermore, the LSB steganography technique effectively concealed the encryption key without causing noticeable changes to the image, making it difficult for attackers to detect or extract the key.

6. References

1. Stallings, W.(2017). Cryptography and Network Security: Principles and Practice. Pearson Education. A comprehensive guide to cryptographic algorithms and network security principles.

2. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

- Detailed explanation of the AES algorithm and its design.

3. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

- A classic book covering various cryptographic algorithms and their applications.

4. Patel, R., & Patel, S. (2016). Hybrid Cryptography for Secure Communication. International Journal of Computer Applications.

- Discusses the effectiveness of hybrid cryptography in secure communication.

5. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital Image Steganography: Concepts and Applications. IEEE Transactions onInformation Forensics and Security.

- Explores steganography techniques, including LSB, for secure data hiding.