A PROJECT REPORT

on

"Data Security Using Cryptography and Steganography"

Submitted to

KIIT Deemed to be University

In Partial Fulfillment of the Requirement for the Award of

BACHELOR'S DEGREE IN INFORMATION TECHNOLOGY

BY

Rakesh Kumar	**2129144**
Tushar bhatt	**2129119**
Vishes Raj Solanki	**2129124**
Avi Bhagat	**2129062**
Rahul Bagaria	**2129140**

UNDER THE GUIDANCE OF

DR. Dayal Kumar Behera

SCHOOL OF COMPUTER ENGINEERING

KALINGA INSTITUTE OF INDUSTRIAL TECHNOLOGY

BHUBANESWAR, ODISHA -751024

APRIL 2024

KIIT Deemed to be University

School of Computer Engineering
Bhubaneswar, ODISHA 751024

CERTIFICATE

This is certify that the project entitled

"Data Security Using Cryptography and Steganography"

Submitted by

Rakesh Kumar	2129144
Tushar bhatt	2129119
Vishesh Raj Solanki	2129124
Avi Bhagat	2129062
Rahul Bagaria	2129140

is a record of bonafide work carried out by them, in the partial fulfillment of the requirement for the award of Degree of Bachelor of Engineering (Computer Sci-ence & Engineering OR Information Technology) at KIIT Deemed to be university, Bhubaneswar. This work is done during the year 2022-2023, under our guidance.

Date: 09/04/2024

DR. Dayal Kumar Behera
Project Guide

Acknowledgements

We are profoundly grateful to **DR. DAYAL KUMAR BEHERA** of **Affiliation** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion .

We would like to express our heartfelt gratitude to all those who contributed to the successful completion of our project on "Data Security Using Cryptography and Steganography." This project would not have been possible without the support, guidance, and encouragement of various individuals and organizations.

.We are also grateful to our academic institution KIIT UNIVERSITY for providing us with the necessary resources, facilities, and conducive learning environment to undertake this project. The infrastructure and technical support offered by the institution were instrumental in our project's execution.

Additionally, we would like to acknowledge the authors of the various research papers, articles, and textbooks that served as valuable sources of information and inspiration for our project. Their contributions to the field of data security and steganography laid the foundation for our work.

In conclusion, we acknowledge and appreciate the contributions of all those who played a role, big or small, in the successful completion of this project. Their support and guidance have been instrumental in shaping our learning experience and professional growth.

Thank you.

Raksesh Kumar
Tushar Bhatt
Vishesh Raj Solanki
Avi Bhagat
Rahul Bagaria

ABSTRACT

Data masking is essential for avoiding data tampering and safeguarding the security and integrity of the information that will be delivered. An adversary exploits another person's data for personal benefit in addition to their own objectives. Data hiding is mostly used to protect information from outsiders who might misuse it. Data hiding is a technique that can be applied in many ways to safeguard and secure data during transmission. The two methods of data hiding that make up the five are steganography and encryption. With this project, users can choose from a range of techniques to conceal data for any kind of media, including audio. Data integrity, confidentiality, and authenticity are critical in today's world of digital communication. This study investigates the combination of steganography and cryptography methods as a strong approach to improve data security in contemporary information systems. The work investigates the synergistic application of steganographic techniques like spread spectrum techniques and LSB embedding with cryptographic algorithms like AES and RSA to strengthen data against unauthorized access and detection. This study attempts to shed light on the relative effectiveness of different strategies in protecting sensitive data from cyberattacks by analysing their advantages and disadvantages.

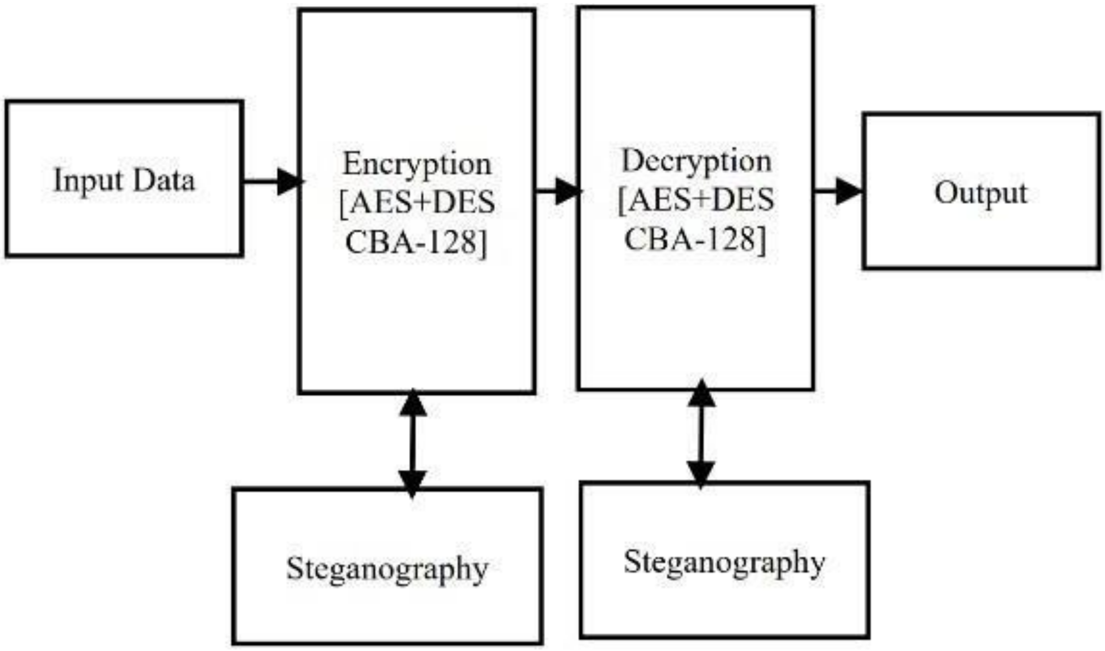
Keywords:
**Data security,
cryptography,
steganography,
AES, RSA, LSB embedding,
spread spectrum, information systems,
cyber threats, confidentiality**

Contents

Chapter 1

Introduction

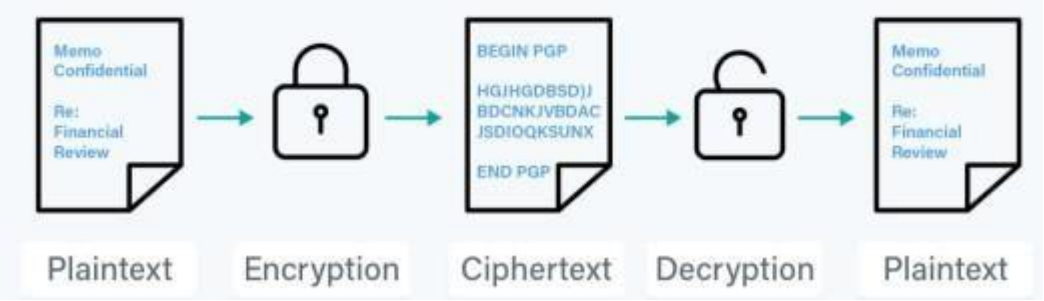
An illustration of a computer screen showing private financial data emphasizes the necessity of strong encryption methods to prevent data breaches and unwanted access. A graphic that highlights the growing frequency of cyberattacks that target sensitive data and emphasizes the need for advanced security methods like steganography and cryptography. An illustration of a hacker trying to obtain private data by intercepting communication channels highlights how important encryption is to maintaining data integrity and secrecy. Diagram demonstrating the need for steganographic techniques to conceal data within innocent files and the susceptibility of typical file storage methods to unauthorized access.



Chapter 2

Basic concepts:

Cryptography: Since the beginning of time, cryptography techniques have been used to guarantee the confidentiality of communications between parties. Using an appropriate key, this method—also referred to as the "art of information hiding"—encrypts plaintext into ciphertext before sending it to the other parties over an unsecure channel. By applying a secret key to decrypt the ciphertext, the original plaintext can be retrieved. Without knowing the key, plaintext cannot be decrypted. Among the many aspects in which cryptography is essential are authentication, confidentiality, secrecy, nonrepudiation, and key exchange.

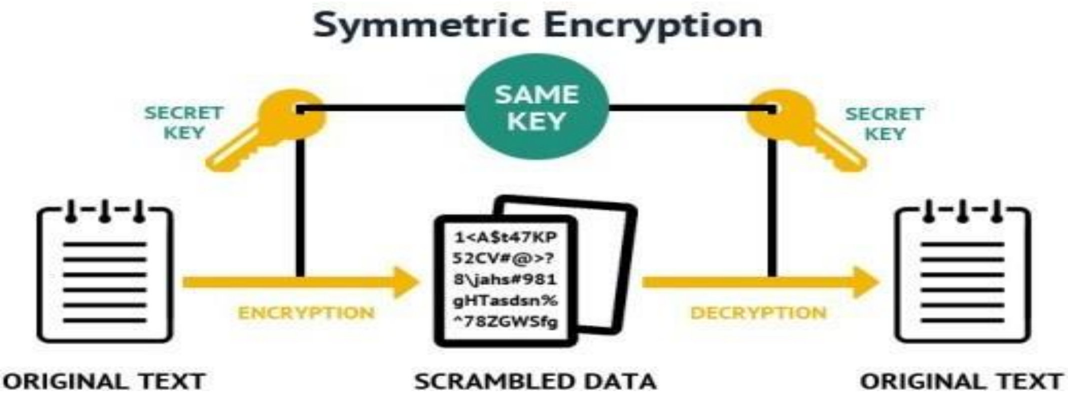


Symmetric Key Cryptography:

The terms symmetric-key, shared-key, single-key, and finally private-key encryption are occasionally used to describe the secret key encryption technique.

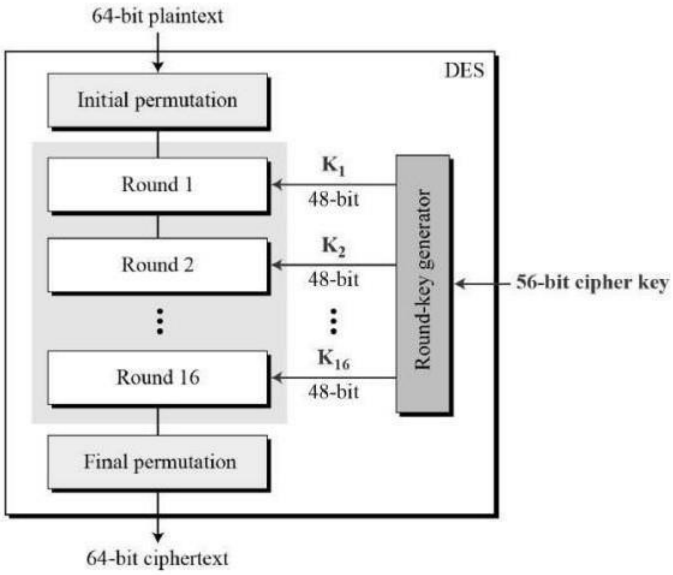
The private key mechanism is used by all parties to encrypt and decrypt secret data. The original data, or plaintext, is encrypted by the transmitter using a key, and the plaintext is obtained by the recipient using a key to decrypt a message. The key will only be accessible to those who are authorized to encrypt or decode data.

There is an issue with key distribution even though the technique offers sufficient transmission security. If someone finds the key or steals it, they can readily acquire all of the data. One example of a symmetric-key is the DES Algorithm.



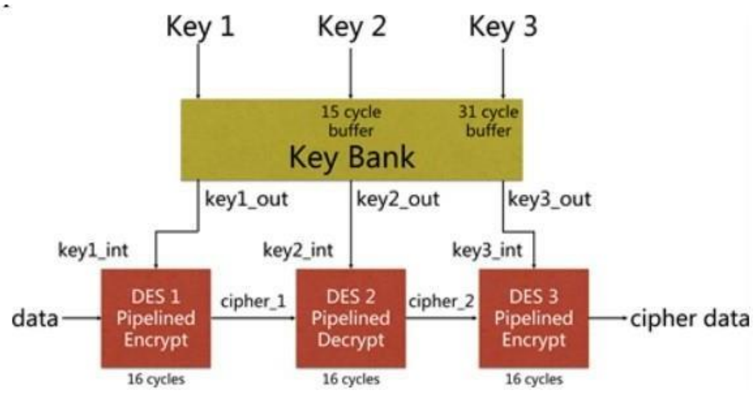
DES:

The symmetric-key algorithm DES uses a Feistel network as its foundation. The fact that the same key is used for both encryption and decryption make it a symmetric key cipher. The resulting method is easier to employ because both procedures are almost identical because of the Fehling network. The real security provided by the key is only 56 bits, even if the DES block and key sizes are both 64 bits.



Triple DES:

The shorter key length of DES led to the creation of 3DES as a more secure substitute. The DES algorithm is performed three times with three different keys in 3DES; however, it is only deemed secure when three different keys are used. A symmetric-key block cipher, the Triple Data Encryption method (also known as Triple DEA, Triple DEA, Triple DES (3DES, or TDES) encrypts each data block using the DES cypher method three times.



Steganography

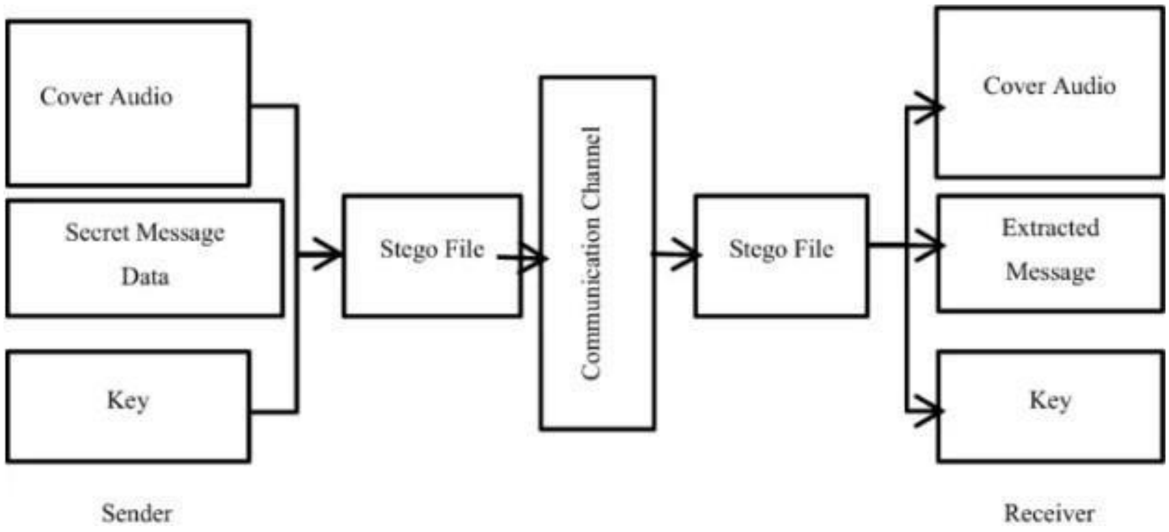
Its focus may be defined as the science of hiding and sending data over supposedly reliable carriers in an attempt to disguise the data's presence. As so, the message's existence was never established in the first place. If someone looks at the cover where the data is buried, they won't attempt to decode it because they won't be aware that there is any covering data there.

The stego system encoder can insert the secret information into the cover medium by using a certain algorithm. The cover object will be referred to as a stego object once the secret data has been implanted in it. By choosing the appropriate channel and using the same stego mechanism, the decoder system obtains the original information that the sender wishes to communicate. This is how the stego object is also sent to the recipient.

Audio Steganography:

An encoded audio file containing a secret message is the aim of audio steganography. Sensitive information can be concealed or transferred safely using this strategy. Confidentiality for private messages may also be ensured if the communication is encrypted.

Images cannot compare to the astonishing capabilities of audio steganography since the Human Auditory System (HAS) has a large range of audible frequencies, powerful hearing, and immense power.



Fernet Algorithm:

Simultaneous encryption and data authentication are offered by the Fernet algorithm. The Python Cryptographic Authority (PYCA) develops the cryptography library for Python, which includes this particular component.Old keys can be easily replaced because it rotates the keys and immediately creates a new ferrnet key. Therefore, in order to begin encrypting new messages, we can include your new key at the top of the list and delete older keys that are no longer needed.Thus, it assists in data security without posing any of the hazards associated with using cryptographic primitives on your own.

Chapter 3

Problem Statement / Requirement Specifications

Problem Statement:

With the help of audio steganography and TDES, our program will increase the security of the data that is on the network and is being transferred from the sender to the recipient.
The only people on the network will be the authorized users, or those who are utilizing our program. The recommended method is to successfully conceal the textual data in an audio file so that it cannot be suspected that it is hidden in the picture.
Its purpose is to prevent the attacks by employing a unique, non-comparable carrier file.
The project's objective is to hide data in audio while maintaining the quality of data concealment using steganography. We employed a method for concealing the data in a different audio file so that it could be safely transferred across the network without anyone seeing that it was concealed.
This method will protect the data even if it requires a unique audio that we can use as a carrier and disguise the data that is well within the audio's ability to conceal.

3.1 Project Planning

Steps to be Followed in Project Execution

1. Requirement gathering: Get all the information you need from stakeholders about the limitations, needed functionalities, and data security needs.
2. Feasibility Study: Evaluate whether using cryptography and steganography techniques is feasible, taking into account the project's timeframe, technological know-how, and available resources.
3. Define the project's scope, including the precise steganography methods (audio steganography) and encryption algorithms (DES, Triple DES) that will be used.

The fourth step in project development is resource allocation. This involves allocating hardware, software, and human resources.

5. Timeline Planning: Create a project schedule that includes deliverables and milestones to guarantee that each phase is finished on schedule.6. Risk Assessment: Determine possible project risks, such as resource limitations, technological difficulties, and security flaws, and create plans to mitigate them.

7.Quality Assurance Plan: Establish procedures for quality assurance to guarantee that the program complies with established guidelines and specifications.

3.2 Project Analysis

After collecting requirements and conceptualizing the problem statement, thorough analysis is conducted to identify any ambiguities, inconsistencies, or mistakes. This analysis involves:

Requirement Review: Check that the requirements gathered are precise, comprehensive, and in line with the demands of the stakeholders. Risk analysis involves evaluating the possible hazards related to the project specifications and pinpointing any ambiguities or potential problems.

Feasibility Analysis: Determine if it is technically, financially, and operationally feasible to implement the suggested solution within the specified parameters.

Gap Analysis: Find any inconsistencies or gaps between the specifications and the suggested solution, then devise plans of action to fix them.

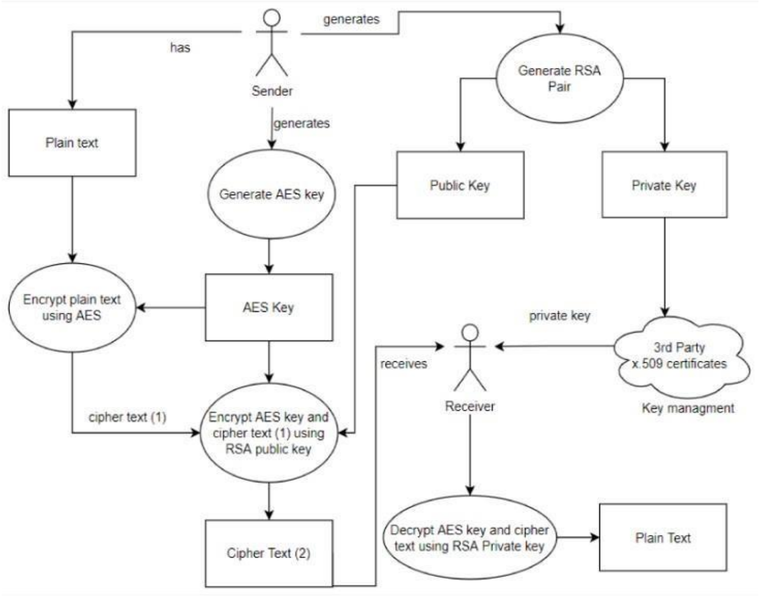
3.3 System Design

3.3.1 Design Constraints

The working environment for the project includes:

- Software: Development environment should support programming languages and libraries for implementing cryptography algorithms (e.g., Python with cryptography library).
- Hardware: Sufficient computational resources for cryptographic operations, including CPU and memory.
- Experimental Setup: Access to audio recording and playback devices for testing audio steganography techniques.

3.3.2 System Architecture OR Block Diagram



Chapter 4

Implementation

4.1 Methodology

The Triple DES algorithm and steganography are the foundation of our two-way encryption paradigm.

Encryption process:

- Encrypt text using steganography into an audio file.
- Apply Triple DES Algorithm to encrypt the audio file for additional security.
- Sender's role:

Possesses Triple DES Key.

- Sends the encrypted audio file to chosen recipient.
- Recipient's role:

Receives the encrypted audio file.

- Utilizes Triple DES Key to decrypt the audio file.
- Extracts concealed text message using steganography.
- Receives decrypted text message after successful decryption.

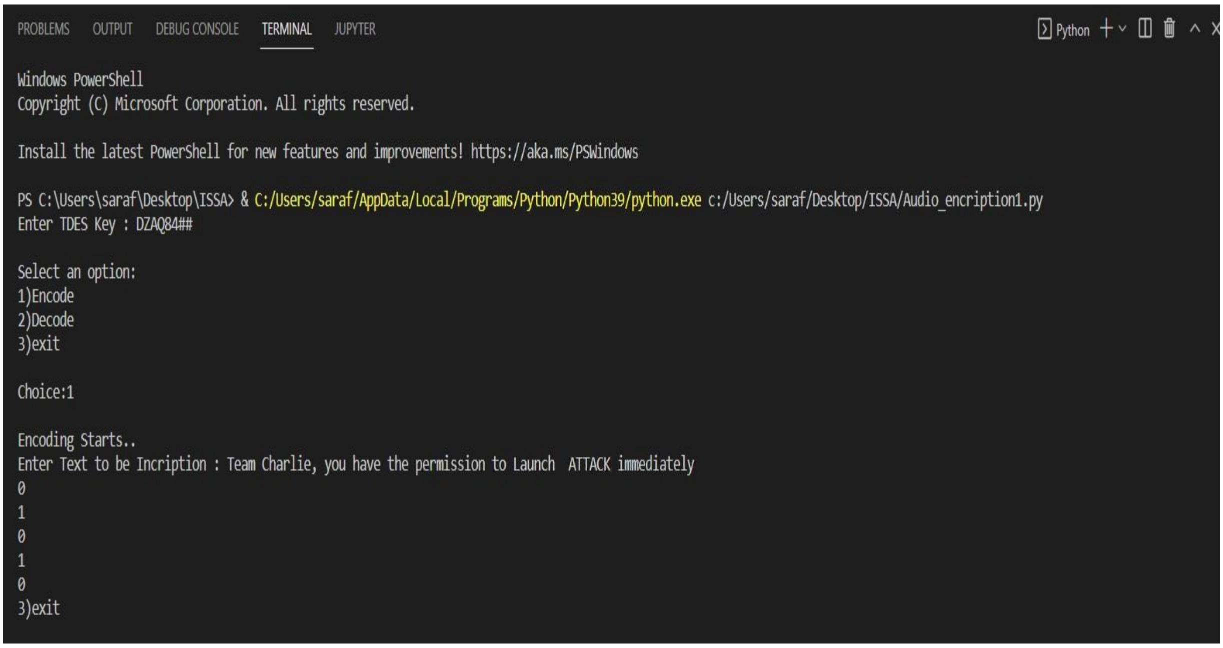
4.2 Testing OR Verification Plan

Test ID	Test Case Title	Test Condition	System Behavior	Expected Result
T01	Encryption Process	Text to be encrypted is provided. Triple DES key is available for encryption. Audio file is selected as the carrier for steganography.	Text is encrypted using Triple DES algorithm. Encrypted text is embedded into the selected audio file using steganography.	Text is successfully encrypted using Triple DES algorithm. Encrypted text is hidden within the audio file without affecting its quality or integrity.
T02	Decryption Process	Encrypted audio file is provided. Triple DES key is available for decryption.	Audio file is decrypted using Triple DES algorithm. Encrypted text is extracted from the decrypted audio file using steganography.	Audio file is successfully decrypted using Triple DES algorithm. Encrypted text is extracted from the decrypted audio file without any loss or corruption.

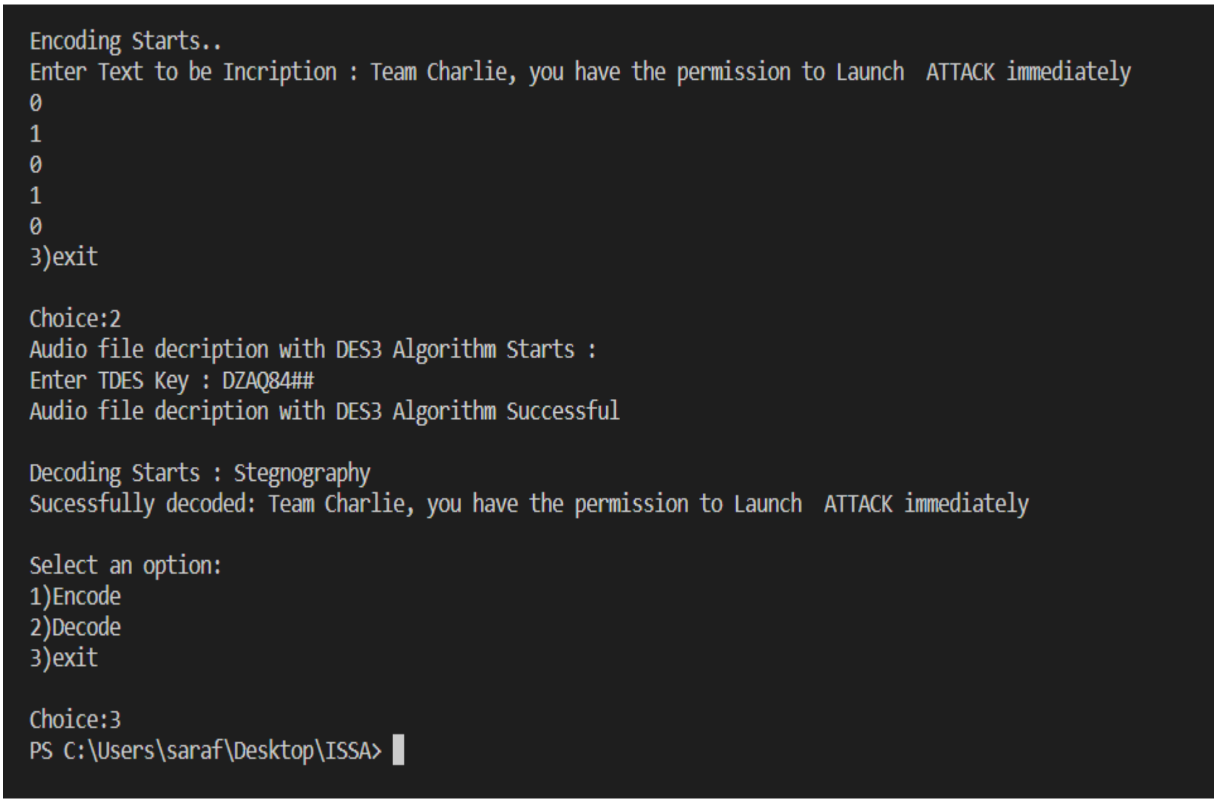
T03	Data Integrity Verification	Original text and decrypted text are available.	Original text and decrypted text are compared for consistency and accuracy.	Decrypted text matches the original text, ensuring data integrity and successful decryption.

4.3 Result Analysis

Output
Steganography and Triple DES Algorithm

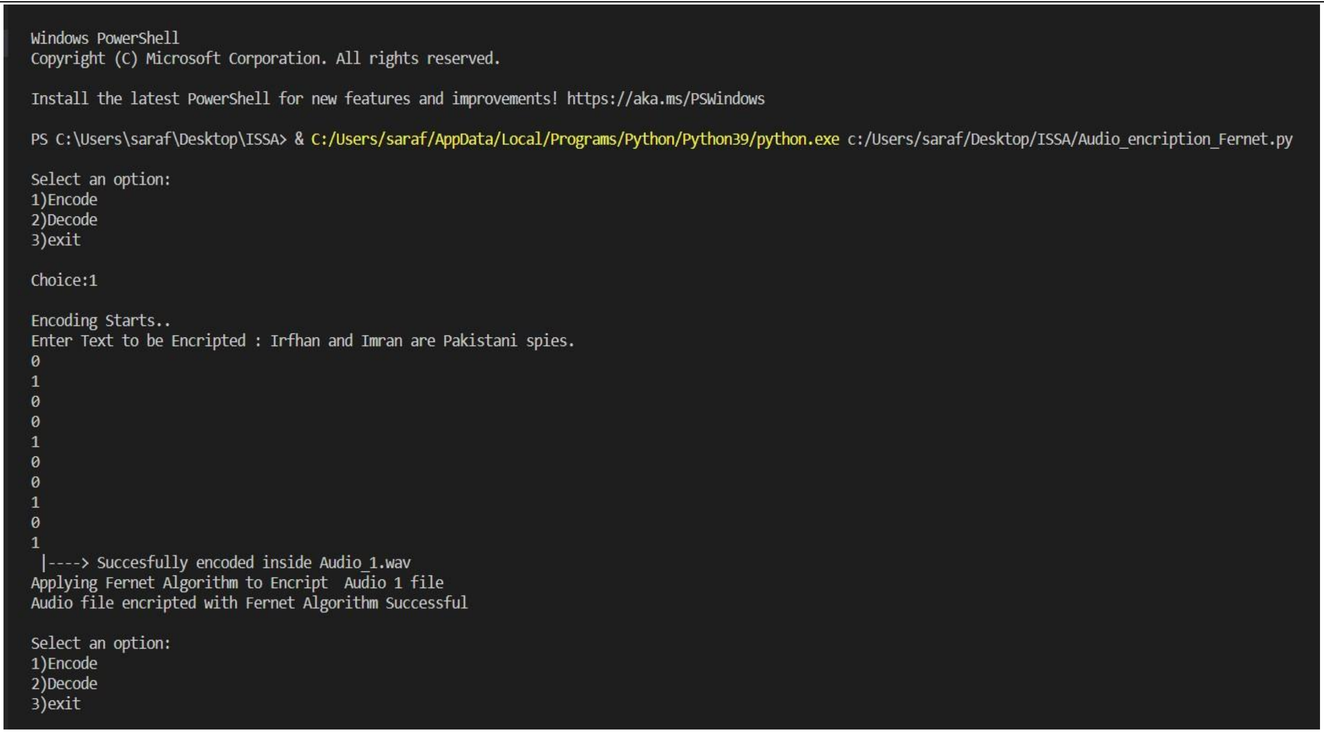


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\saraf\Desktop\ISSA> & C:/Users/saraf/AppData/Local/Programs/Python/Python39/python.exe c:/Users/saraf/Desktop/ISSA/Audio_encription1.py
Enter TDES Key : DZAQ84##

Select an option:
1)Encode
2)Decode
3)exit

Choice:1

Encoding Starts..
Enter Text to be Incription : Team Charlie, you have the permission to Launch  ATTACK immediately
0
1
0
1
0
3)exit
```

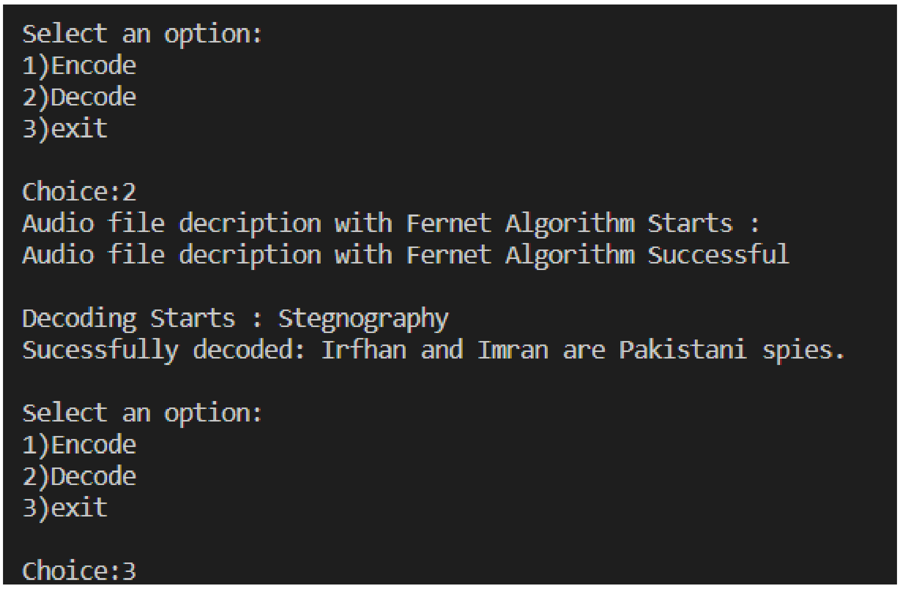


```
Encoding Starts..
Enter Text to be Incription : Team Charlie, you have the permission to Launch  ATTACK immediately
0
1
0
1
0
3)exit

Choice:2
Audio file decription with DES3 Algorithm Starts :
Enter TDES Key : DZAQ84##
Audio file decription with DES3 Algorithm Successful

Decoding Starts : Stegnography
Sucessfully decoded: Team Charlie, you have the permission to Launch  ATTACK immediately

Select an option:
1)Encode
2)Decode
3)exit

Choice:3
PS C:\Users\saraf\Desktop\ISSA>
```

Output Steganography and Fernet Algorithm



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\saraf\Desktop\ISSA> & C:/Users/saraf/AppData/Local/Programs/Python/Python39/python.exe c:/Users/saraf/Desktop/ISSA/Audio_encription_Fernet.py

Select an option:
1)Encode
2)Decode
3)exit

Choice:1

Encoding Starts..
Enter Text to be Encripted : Irfhan and Imran are Pakistani spies.
0
1
0
0
1
0
0
1
0
1
 |----> Succesfully encoded inside Audio_1.wav
Applying Fernet Algorithm to Encript  Audio 1 file
Audio file encripted with Fernet Algorithm Successful

Select an option:
1)Encode
2)Decode
3)exit
```



```
Select an option:
1)Encode
2)Decode
3)exit

Choice:2
Audio file decription with Fernet Algorithm Starts :
Audio file decription with Fernet Algorithm Successful

Decoding Starts : Stegnography
Sucessfully decoded: Irfhan and Imran are Pakistani spies.

Select an option:
1)Encode
2)Decode
3)exit

Choice:3
```

Chapter 5

Standards Adopted

5.1 Design Standards

Modular Architecture: Employ a modular architecture where distinct modules handle encryption, decryption, steganography, key management, and user interface functionalities. This approach promotes code reusability, maintainability, and scalability.

Layered Design: Implement a layered design architecture with clear separation between the presentation layer (user interface), business logic layer (encryption, decryption, steganography), and data access layer (key management). This separation ensures that each layer focuses on its specific responsibilities, facilitating easier debugging and future enhancements.

Secure Communication Channels: Design secure communication channels between modules to prevent unauthorized access or interception of sensitive data during transmission. Use secure protocols such as HTTPS or SSL/TLS for communication between client and server components.

Secure Key Management: Implement robust key management practices, including secure key generation, storage, transmission, and disposal. Utilize secure cryptographic key storage mechanisms such as key vaults or hardware security modules (HSMs) to protect cryptographic keys from unauthorized access.

Adherence to Cryptographic Standards: Ensure that cryptographic algorithms used in the project adhere to industry-standard encryption protocols and recommendations (e.g., AES for symmetric encryption, RSA or ECC for asymmetric encryption). Avoid using deprecated or insecure cryptographic algorithms.

Scalability and Performance: Design the system to be scalable and performant, capable of handling increasing volumes of data and user requests without sacrificing security. Employ efficient cryptographic algorithms and data processing techniques to minimize computational overhead and response times.

Error Handling and Logging: Implement comprehensive error handling mechanisms to detect and handle exceptions gracefully. Integrate logging functionality to record important security events, errors, and audit trails for forensic analysis and compliance purposes.

Cross-Platform Compatibility: Ensure that the software solution is cross-platform compatible, capable of running seamlessly on different operating systems and environments. This enhances flexibility and interoperability across diverse deployment scenarios.

Usability and Accessibility: Design the user interface to be intuitive, user-friendly, and accessible to a wide range of users, including those with disabilities. Incorporate accessibility features such as keyboard navigation and screen reader compatibility to improve usability for all users.

Documentation and Compliance: Document the design architecture, implementation details, and security considerations comprehensively. Ensure compliance with relevant security standards, regulations, and best practices (e.g., NIST guidelines, GDPR) throughout the design and development process.

5.2 Coding Standards

Our development approach adheres to industry-standard coding practices and security principles to ensure the reliability, maintainability, and security of the software:

- Utilize established cryptographic libraries and APIs for implementing encryption algorithms.
- Follow secure coding practices to mitigate common vulnerabilities such as injection attacks and buffer overflows.
- Implement robust key management procedures to ensure secure key generation, storage, transmission, and disposal.
- Validate and sanitize input data to prevent injection attacks and ensure the integrity of cryptographic operations.
- Conduct thorough code reviews to identify and rectify security flaws and vulnerabilities.
- Document the code comprehensively, including explanations of cryptographic algorithms used and key management procedures.
- Implement comprehensive testing procedures, including unit tests, integration tests, and security tests, to verify correctness and security.

5.3 Testing Standards

For testing and verification of the project work on data security using cryptography and steganography, the following ISO and IEEE standards are adhered to:

ISO/IEC 25010: Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models: This standard provides a framework for specifying, evaluating, and managing software quality. It covers quality characteristics such as functional suitability, performance efficiency, security, and maintainability, which are essential for ensuring the effectiveness and reliability of the project.

ISO/IEC 27001: Information security management systems - Requirements: This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Adhering to this standard ensures that the project follows best practices for information security governance, risk management, and compliance.

IEEE 1012: Standard for Software Verification and Validation: This standard provides guidelines for the verification and validation of software products and systems. It covers processes, activities, and tasks related to software testing, inspection, and analysis to ensure that software products meet specified requirements and quality standards.

IEEE 1028: Standard for Software Reviews and Audits: This standard defines the processes and procedures for conducting software reviews and audits throughout the software development lifecycle. It includes guidelines for conducting formal reviews, inspections, walkthroughs, and audits to identify defects, improve quality, and ensure compliance with requirements.

ISO/IEC/IEEE 29119: Software and systems engineering -- Software testing: This standard provides a comprehensive framework for software testing processes, activities, and techniques. It covers topics such as test planning, test design, test execution, and test management, helping to ensure thorough and systematic testing of the project.

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

To sum up, the project's goal was to improve data security over networks by combining Triple Data Encryption Standard (TDES) encryption and audio steganography. The major objective was to successfully hide textual information inside audio files so that the information would stay hidden, and the audio would not be compromised.

The project addressed the need for clandestine communication without raising red flags by concentrating on steganography as a method of data concealing. Using a different carrier file that isn't the same as the original audio provides an additional degree of protection against possible hacks.

The focus of the project was always on protecting data while it was being transmitted over networks, making sure that only people with permission and the appropriate application could view and deal with the hidden data. This methodology reduces the potential for unwanted access and interceptions of confidential information.

The use of TDES encryption strengthened data security even more by guaranteeing that, in the unlikely event that the data was uncovered, it would still be encrypted and unintelligible to outsiders.

With the smooth integration of audio steganography and TDES encryption, the project effectively met its overall goal of enhancing data security. A more secure and robust network environment is created by the methods used, which guarantees that data is secured throughout transmission. The protection of sensitive data in an increasingly linked world may be facilitated by future developments in data security technology brought about by ongoing research and development in this field.

6.2 Future Scope

The current research has succeeded in improving data security by using TDES encryption and audio steganography, however there are still several areas that could be investigated and improved in the future:

Sophisticated Steganographic Methods: Investigate and create sophisticated steganographic methods to enhance the strength and efficiency of data hiding in audio recordings. Investigate methods like spread spectrum modulation, frequency domain embedding, and adaptive steganography to improve concealment and thwart detection attempts.

Integration with Emerging Technologies: Explore integration with emerging technologies such as artificial intelligence (AI) and machine learning (ML) to enhance the security and efficiency of data concealment and encryption algorithms. Utilize AI/ML algorithms for optimizing carrier selection, payload encoding, and encryption key generation.

Enhanced Authentication Mechanisms: Implement advanced authentication mechanisms to ensure the authenticity and integrity of authorized users accessing the network. Explore the use of biometric authentication, multi-factor authentication (MFA), and blockchain-based authentication to strengthen access control measures.

Optimization for Real-Time Communication: Make the system as efficient as possible for situations requiring high throughput and low latency, such as video conferences and voice calls. Provide effective protocols and methods to enable real-time data extraction and embedding in audio streams while maintaining performance and quality.

Cross-Platform Compatibility: Increase the application's compatibility to accommodate a greater variety of platforms and gadgets, such as web browsers, mobile devices, and Internet of Things gadgets. To facilitate seamless integration with a variety of operating systems and contexts, create native applications and browser extensions.

Improved User Experience: Make the program more user-friendly by adding interactive feedback systems, easy-to-use controls, and user-friendly interfaces. Find out where things need to be improved and refined by doing usability testing and getting user feedback.

Scalability and Performance Optimization: Enhance the system's performance and scalability to manage increasing user traffic and data quantities. To maximize resource consumption and improve overall system efficiency, put caching systems, load balancing measures, and distributed processing approaches into practice.

Through the pursuit of these avenues for future development and innovation, the project will be able to adapt and change in response to the ever-changing demands and challenges associated with data security in contemporary networks. We may further improve the efficacy and robustness of data security systems based on audio steganography and encryption techniques by continued study, experimentation, and cooperation.

References

[1] Jayaram, Ranganatha, & Anupama. (2011). Information Hiding Using Audio Steganography - A Survey. The International journal of Multimedia & Its Applications, 3, 86-96. doi: 10.5121/ijma.2011.3308.

[2] Kamred Udham Singh. Article: A Survey on Audio Steganography Approaches. International Journal of Computer Applications, 95(14), 7-14 (June 2014).

[3] Shi, C., & Bhargava, B. (1998). Light-weight MPEG Video Encryption Algorithm. In Proceedings of the International Multimedia Conference on Multimedia, (Multimedia98, Shaping The Future) (pp. 55-61, January 23-25). New Delhi, India: IETE, Tata McGraw-Hill Publishing Company.

[4] Zheng Liu, Xue Li. Motion Vector Encryption in Multimedia Streaming. Proceedings of the 10th International Multimedia Modeling Conference (IEEE 2004).

[5] T. Vino, E. Logashanmugam. A Modelbased Multimedia Encryption Scheme for Real Time Videos (IEEE 2010).

[6] Wenjun Zeng, Shawmin Lei. Efficient frequency domain selective scrambling of digital video (In Proc. of the IEEE Transactions on Multimedia, 2002, pp. 118–129).

[7] Raphael Horvath, D. N. (2015). A Literature Review on Challenges and Effects of Software Defined Networking. Conference on ENTERprise Information Systems / International Conference on Project. Elsevier ScienceDirect Procedia Computer Science. doi: 10.1016/j.procs.2015.08.563

[8] A discussion with Amin Vahdat, D. C. (2016, March). A Purpose-Built Global Network: Google's move to SDN. Communications of the ACM, 59(3), 46-54. doi: DOI:10.1145/2814326

[9] H. Li, P. L. (2014). Byzantine-resilient secure software defined networks with multiple controllers. Communications (ICC), IEEE International Conference, 695-700.

[10] Aditya Kotkar, Shreyas Khadapkar, Aniket Gupta, Smita Jangale, "Multiple layered Security using combination of Cryptography with Rotational, Flipping Steganography and Message Authentication", 2022 IEEE International Conference on Data Science and Information System (ICDSIS), pp.1-5, 2022.

[11] Putta Bharathi, Gayathri Annam, Jaya Bindu Kandi, Vamsi Krishna Duggana, Anjali T., "Secure File Storage using Hybrid Cryptography", 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp.1-6, 2021.

[12] Yue Zhao, Leyu Lin, Yiru Niu, Kaijun Wu, Yao Hao, Hong Su, Yarang Yang, "The Secure Computing Architecture for Dual Hard Disk and Dual System Switching", 2022 IEEE 5th International Conference on Big Data and Artificial Intelligence (BDAI), pp.125-129, 2022.

[13] Rini Indrayani, "Modified LSB on Audio Steganography using WAV Format", 2020 3rd International Conference on Information and Communications Technology (ICOIACT), pp.466-470, 2020.

[14] Artz, D. (2001). Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal, (June).

[15] Moerland, T. (2001). Steganography and Steganalysis. Leiden Institute of Advanced Computing Science. Accessed September 12, 2012. Available from www.liacs.nl/home/tmoerl/privtech.pdf

[16] Chandramouli, R., Kharrazi, M., & Memon, N. (2003). Image steganography and steganalysis: Concepts and Practice. Proceedings of the 2nd International Workshop on Digital Watermarking, October.

[17] Sumartono, Isnar, Siahaan, Andysah Putera Utama, & Arpan, Arpan.

[18] Dhany, Hanna & Izhari, Fahmi & Fahmi, Hasanul & Tulus, Tulus & Sutarman, Mr. (2018). Encryption and Decryption using Password Based Encryption, MD5, and DES. 10.2991/icoposdev-17.2018.57.

Data Security Using Cryptography and Steganography

Abstract: Data masking protects sensitive information during transfer by disguising it. This project lets users choose algorithms to hide data (like in audio) using techniques like encryption to prevent unauthorized access.

Individual Contribution and Findings

Student 1: [Rakesh Kumar 2129144]

Role in Project Group:

In our project group focusing on "Data Security Using Cryptography and Steganography," my role primarily centered around cryptography implementation. I was responsible for researching cryptographic algorithms, implementing encryption and decryption functions, and ensuring the secure transmission and storage of sensitive data.

Planning Involved:

To implement my part effectively, I began by conducting an in-depth analysis of various cryptographic algorithms and their suitability for our project requirements. Following this, I collaborated with the team to identify the specific data encryption needs and design the encryption process flow. I then proceeded to implement the chosen algorithms, considering factors such as key management, data integrity, and performance.

Individual Contribution to Project Report Preparation:

For the project report, I contributed to the chapters related to cryptography implementation and data security. I documented the cryptographic algorithms used, including their theoretical background, implementation details, and security considerations. Additionally, I provided insights into encryption key management practices and data protection strategies, ensuring a comprehensive understanding for readers.

Individual Contribution for Project Presentation and Demonstration:

In the project presentation and demonstration, I played a crucial role in showcasing the cryptography implementation and its impact on data security. I prepared slides explaining the encryption process and its significance in protecting sensitive information. During the demonstration, I demonstrated the encryption and decryption functionalities, highlighting the effectiveness of our cryptographic solution in securing data transmission and storage.

Full Signature of Supervisor: Full signature of the student:

……………………………. ……………………………..

Student 2: [Tushar Bhatt 2129118]

Role in Project Group:

In our project group focusing on "Data Security Using Cryptography and Steganography," my role primarily revolved around steganography implementation. I was responsible for researching steganographic techniques, embedding data into digital media, and ensuring covert communication channels for secure data transmission.

Planning Involved:

To implement my part effectively, I started by researching various steganographic algorithms and their applicability to our project objectives. I then collaborated with the team to define the data hiding requirements and design the embedding process. Following this, I implemented the chosen steganographic techniques, considering factors such as payload capacity, imperceptibility, and robustness against detection.

Technical Findings and Experience:

During the implementation phase, I encountered challenges related to balancing data embedding capacity with image quality degradation. Through experimentation with different embedding methods and payload sizes, I gained insights into optimizing the trade-off between data capacity and visual impact. Additionally, I learned about steganalysis techniques and countermeasures to detect and mitigate steganographic attacks, enhancing my understanding of covert communication security.

Individual Contribution to Project Report Preparation:

For the project report, I contributed to the chapters related to steganography implementation and covert communication. I documented the steganographic algorithms employed, detailing the embedding process and its impact on digital media. Additionally, I provided insights into steganalysis techniques and mitigation strategies, ensuring a comprehensive overview of covert communication security.

Individual Contribution for Project Presentation and Demonstration:

In the project presentation and demonstration, I played a crucial role in showcasing the steganography implementation and its implications for data security. I prepared slides illustrating the data embedding process and its effectiveness in hiding sensitive information. During the demonstration, I demonstrated the embedding and extraction functionalities, highlighting the covert nature of our communication channels and their resistance to detection.

Full Signature of Supervisor: Full signature of the student:

……………………………. ……………………………..

Student 3: [Avi Bhagat 2129062]

Role in Project Group:

Within our project group centered on "Data Security Using Cryptography and Steganography," my primary responsibility was the implementation of cryptographic solutions. This included researching various cryptographic algorithms, developing encryption and decryption functionalities, and ensuring the secure handling of confidential data.

Planning Involved:

To effectively execute my role, I conducted an extensive analysis of cryptographic algorithms to determine their suitability for our project's objectives. Collaborating with the team, we defined the encryption requirements and designed the encryption workflow, considering aspects like key management and data integrity.

Individual Contribution to Project Report Preparation:

In the project report, my contributions focused on documenting the cryptographic algorithms utilized, their theoretical foundations, implementation details, and security implications. Additionally, I addressed encryption key management strategies and data protection measures to provide a comprehensive overview for readers.

Individual Contribution for Project Presentation and Demonstration:

During the project presentation and demonstration, I played a pivotal role in elucidating the cryptography implementation and its significance in bolstering data security. I created informative slides explaining the encryption process and its impact on safeguarding sensitive data. Through live demonstrations, I showcased the encryption and decryption capabilities, highlighting the efficacy of our cryptographic approach in ensuring secure data transmission and storage.

Full Signature of Supervisor: Full signature of the student:

……………………………. ……………………………..

Student 3: [Rahul Bagaria 2129140]

Role in Project Group:

In our project group focusing on "Data Security Using Cryptography and Steganography," my role primarily centered around project management and coordination. I was responsible for overseeing the project timeline, coordinating tasks among team members, and ensuring timely delivery of project milestones.

Planning Involved:

To effectively manage the project, I started by defining clear project objectives and breaking down tasks into manageable units. I then created a project schedule outlining deadlines and milestones, allocating resources based on individual skills and availability. Throughout the project, I facilitated communication among team members, encouraging collaboration and addressing any issues or concerns promptly.

Technical Findings and Experience:

While my role was primarily focused on project management, I gained insights into various technical aspects of the project through collaboration with team members. I learned about cryptographic and steganographic techniques, their implementation challenges, and their implications for data security. Additionally, I gained experience in version control systems and collaboration tools, enhancing my understanding of project development processes.

Individual Contribution to Project Report Preparation:
For the project report, I contributed to the chapters related to project management and coordination. I documented the project timeline, milestones achieved, and challenges encountered during the development process. Additionally, I provided insights into team dynamics and communication strategies employed, ensuring a comprehensive overview of the project's execution.

Individual Contribution for Project Presentation and Demonstration:

In the project presentation and demonstration, I played a crucial role in organizing and facilitating the presentation session. I ensured that all team members were prepared and allocated time effectively for each segment of the presentation. During the demonstration, I provided context and background information on the project management aspects, highlighting their importance in ensuring project success and delivery.

Each student made significant contributions to different aspects of the project, leveraging their skills and expertise to ensure its successful implementation and delivery.

Full Signature of Supervisor:	Full signature of the student:
…………………………….	……………………………..

Student 3: [Vishesh Raj Solanki 2129124]

Role in Project Group:

Within our project group dedicated to "Data Security Using Cryptography and Steganography," my role revolved around project management and coordination. I took charge of overseeing the project's timeline, coordinating tasks among team members, and ensuring the timely achievement of project milestones.

Planning Involved:

To manage the project effectively, I began by establishing clear project objectives and breaking down tasks into manageable units. I then developed a comprehensive project schedule that outlined deadlines and milestones, allocating resources based on individual skills and availability. Throughout the project, I facilitated open communication among team members, fostering collaboration and addressing any challenges promptly.

Technical Insights and Experience:

During the implementation phase, I encountered challenges related to algorithm selection and implementation complexity. Through rigorous experimentation and testing, I gained valuable insights into the strengths and weaknesses of various cryptographic techniques. This experience enabled me to make informed decisions regarding algorithm choices and understand the importance of robust encryption mechanisms and cryptographic key management practices in ensuring data confidentiality.

Individual Contribution for Project Presentation and Demonstration:

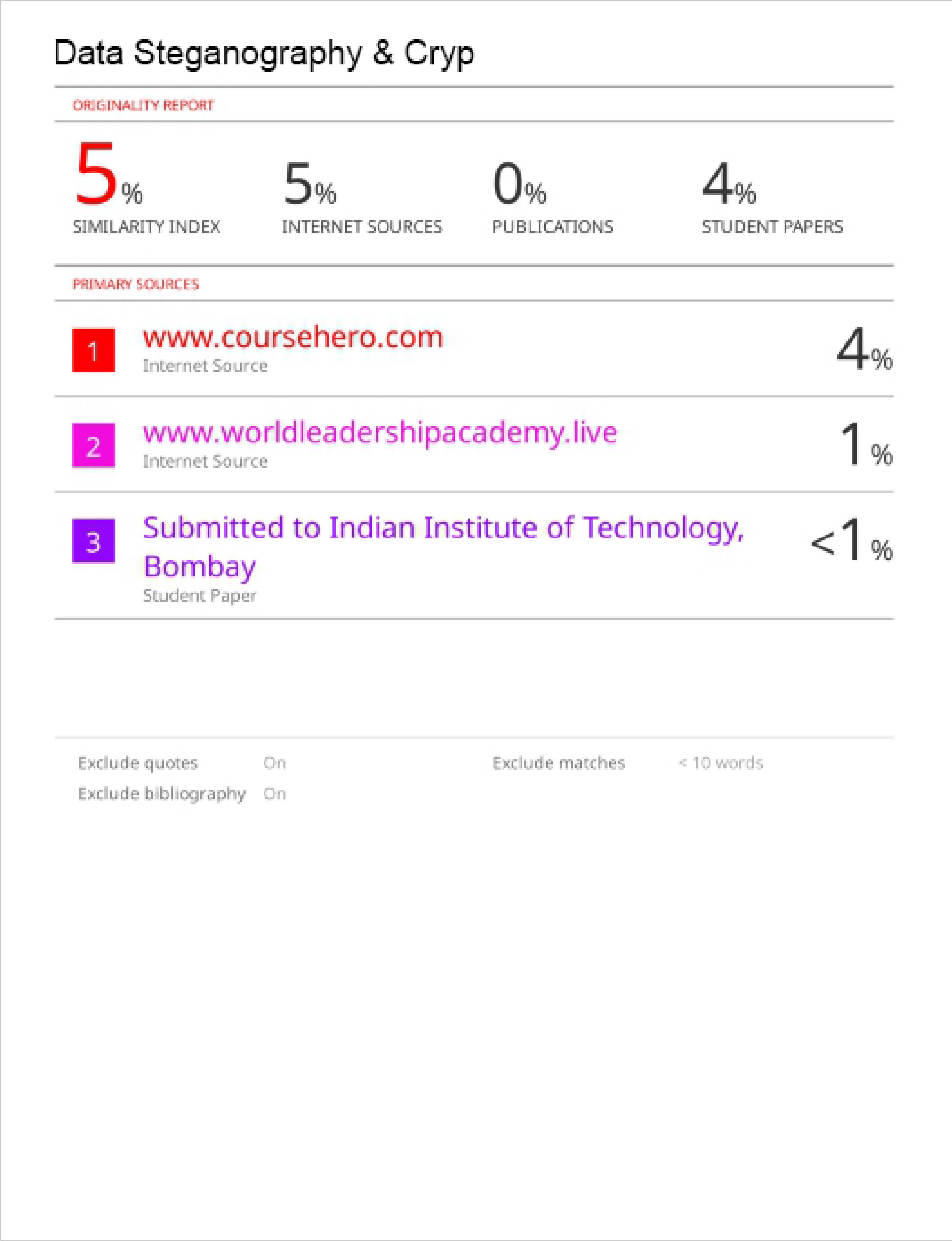
In the project presentation and demonstration, I played a pivotal role in organizing and facilitating the presentation session. I ensured that all team members were well-prepared and allocated time effectively for each segment of the presentation. During the demonstration, I provided context and background information on the project management aspects, emphasizing their significance in ensuring project success and timely delivery.

Each team member contributed significantly to different facets of the project, leveraging their skills and expertise to ensure its successful implementation and delivery..

Full Signature of Supervisor:
…………………………….

Full signature of the student:
……………………………..

Thank You



Data Steganography & Cryp

ORIGINALITY REPORT

5%	5%	0%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	4%
2	www.worldleadershipacademy.live Internet Source	1%
3	Submitted to Indian Institute of Technology, Bombay Student Paper	<1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	On		