



“Steganographic Encryption”

GP Proposal

First Semester - 1446

Prepared by

Student Name	Student ID
Arwa Mesloub	443203895
Yara AlSubhi	443201013
Khlood Aldwayan	443201002
Jana Aljomaih	443200860

Supervised by
Dr. Kholoud Al-saleh



Table Of Contents

1	<i>Introduction</i>	2
2	<i>The Problem</i>	4
3	<i>The Solution</i>	4
4	<i>Product Vision</i>	5
5	<i>Product Roadmap</i>	6
6	<i>Objectives</i>	6
7	<i>Scope</i>	8
8	<i>Hardware/Software Tools and Cost</i>	8
9	<i>Scrum Team</i>	10
	Skill Set Requirements.....	10
	Roles and Responsibilities	10
10	<i>References</i>	11

1 Introduction




Technology has become an essential and important pillar of our lives today, making it easy for us to communicate with the world, learn, and obtain information with ease. However, keeping sensitive information secure has become a major challenge. It wasn't long before encryption became the preferred method for secure communications, evolving from the simple ciphers used in ancient times to the complex encryption algorithms used in modern technology. With the emergence of cyber threats and the increasing sophistication of attackers, traditional encryption alone is no longer enough. While it protects the content of communications, it often fails to hide the fact that communication is taking place, making it a potential target for adversaries.

This loophole has led to the need for newer security measures, with increased requirements. To tackle this challenge, messages must not only be encrypted but also made invisible. Here steganography becomes important. Steganography, which entails secreting information inside what appears to be something innocuous like an image file of no special interest whatsoever, complements encryption by adding an extra layer of security.

The importance of technological solutions in this area is profound both locally and globally. At the local level, businesses and individuals are increasingly vulnerable to cyber threats, which can result in the loss of sensitive data, financial harm, and a breach of privacy. Ensuring that local communities have access to secure communication tools to protect their personal and professional information across the network. On a global scale, the stakes are even higher. International communications, transactions, and collaborations depend on secure channels to prevent spying, fraud, and other malicious activities. As global connectivity increases, so does the need for solutions that can safeguard data across borders and systems, making the development of secure communication technologies a priority for the international community.

Recognizing these vulnerabilities, our ConcealSafe project will try to develop a website application that combines the strengths of both encryption and steganography. Our solution, which encrypts messages and then embeds them into media files, will focus on making communications almost undetectable to unauthorized observers. This approach is twice as secure and private for information sent over insecure channels. In addition, the application will also include advanced security guarantees such as PKI and two-factor authentication. They are there to ensure that not only are messages hidden and encrypted but that they are also protected from being tampered with or accessed by those who should not have access to them.

What we aim to present through this project is a high-security program. In this document, we will thoroughly examine each phase of the project, providing detailed insights into how our website enhances security and ensures effective digital operations.

did  address the domain correctly?

2 The Problem

Exchanging sensitive information over digital channels has become dangerous due to the increasing risks from advancing technology. In addition, there are serious security risks associated with this expansion of data transfer. The existence of messages is usually not hidden by traditional security methods. If the message is visible, it may draw in malicious parties that want to steal and decrypt the data. Due to these channels' lack of privacy, sensitive data is vulnerable to disclosure and is exposed through serious vulnerabilities.

For example, in cases of corporate spying, a company might be exchanging sensitive information over encrypted channels. Competitors or hackers could detect the encrypted traffic and target it with different attacks, knowing that valuable information is being transmitted over that channel. Because of that, the company could suffer financial losses or intellectual property theft. In this case, steganography could have been used to make the communication appear as insensitive data, avoiding suspicion and thus mitigating this kind of attack.

The need for more advanced data security techniques comes from the increasing number of cyberattacks. Current encryption methods are not enough to secure different types of data, including text, videos, audio, files, and images. To enhance protection, information must not only be encrypted but also hidden by using steganography. This need for additional security measures has never been more critical.

3 The Solution

Our project proposes the development of a comprehensive web application that integrates cryptography with steganography to address the security challenges of modern data communication. This dual-layered approach enhances security by not only encrypting messages but also concealing them within various media files, such as text, images, audio, and videos. The key components of our solution include:

1. **Encryption:** Encrypting messages to obscure their meaning.
2. **Steganography:** Embedding these encrypted messages within media files, such as images, audio, or video, making their existence invisible to potential attackers. This covert approach significantly reduces the likelihood of the communication being detected or targeted.
3. **Multi-Factor Authentication:** Implementing multi-factor authentication, including password protection and biometric verification (e.g., fingerprint or face ID), to ensure that only



authorized users can access the hidden messages. This adds an additional layer of security against unauthorized access.

4. **Public Key Infrastructure (PKI):** Utilizing PKI to facilitate the secure sharing of hidden messages, allowing users to exchange encrypted and steganographically hidden messages. This ensures that sensitive data is only accessible to intended recipients.
5. **Diverse Data Handling:** Supporting various forms of data, including text, images, video, and audio, making the application adaptable for different types of sensitive information across multiple sectors.

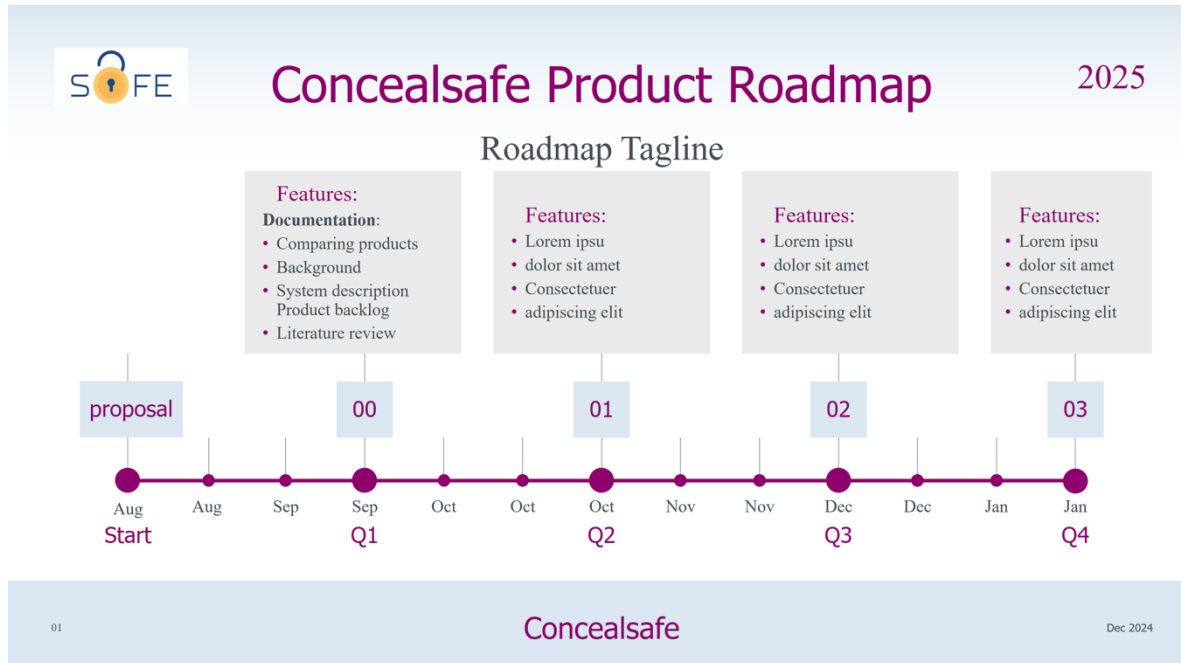
By integrating these methodologies, our project will offer a resilient and confidential communication approach that enhances the security of sensitive information. This methodology overcomes the problems of traditional encryption technologies and offers a reliable way to protect data in our increasingly digital world.

4 Product Vision

For anyone who seeks a robust solution for secure and covert communication of sensitive information, the Consealsafe is a web application that employs an innovative approach by combining cryptography and steganography to guarantee that messages remain private and unreadable from unauthorized parties. Unlike OpenStego, our product is designed to protect and hide various types of information.



5 Product Roadmap



6 Objectives

This project's objectives are structured into Product, Project and Learning Objectives, each serving distinct purposes to guide the development and learning outcomes of the project. These objectives aim to deliver a secure and user-friendly website that implements advanced cryptographic and steganographic techniques for secure communication. Additionally, they emphasize skill enhancement in website app development, security principles, and project management, ensuring a comprehensive learning experience throughout the project lifecycle.

did we write too much of an intro here?

Product Objectives:

- Secure Communication:** Develop a website application that enables secure and covert communication of sensitive messages using cryptography and steganography.
- User-Friendly Interface:** Design an intuitive and easy-to-navigate interface that allows users to encrypt, hide, and share messages seamlessly.
- Enhanced Security methods:** Implement multi-factor authentication and integrate Public Key Infrastructure (PKI) to ensure robust security for message encryption and sharing.
- Efficient Performance:** Optimize the website for efficient encryption, embedding, and retrieval processes to provide a smooth user experience.
- Support for Various Media Types:** Expand steganography to support hiding messages not just in images, but also in audio and video files.



Project Objectives:

1. **Implementation of Cryptography and Steganography:** Develop and integrate algorithms for message encryption and embedding within media files.
2. **User Interface Design:** Create wireframes and prototypes, then implement a user-friendly interface based on design principles and usability testing.
3. **Security Implementation:** Implement multi-factor authentication methods and integrate PKI for secure message sharing.
4. **Understand User Needs:** interview the users and write the user story to figure out the user needs and apply it on the website.
5. **Testing and Validation:** Conduct thorough testing to validate the website's functionality, security features, and performance.
6. **Documentation and User Guide:** Prepare comprehensive documentation outlining the website's architecture, features, and usage instructions.

Learning Objectives:



1. **Understanding Cryptography and Steganography:** Gain deep knowledge of cryptographic algorithms (e.g., AES, RSA) and steganographic techniques for data security and covert communication and how to apply them.
2. **Learning the Skills for Web Application Development:** Enhance our skills in web application development, including UI/UX design and backend integration.
3. **Security Principles:** Learn principles of data security, including encryption, authentication methods, and secure data transmission.
4. **Project Management:** Project Management: Gain experience in planning, implementation, testing, and documenting projects through experimentation during the lifecycle of our project.
5. **Problem-Solving and Innovation:** Apply creative solutions to address challenges in secure communication and enhance the website's functionality and usability.
6. **Group Management and Teamwork:** focus on developing our ability to work collaboratively, communicate effectively, distribute tasks, time management and lead or contribute to group projects efficiently.
7. **Gain more experience with tools:** Gain more experience with Jira as well as GitHub and other software tools.

7 Scope

The project will focus on integrating advanced cryptographic algorithms, such as AES and RSA, to effectively encrypt and obscure message content. Additionally, it will employ steganography techniques to embed these encrypted messages within various media files - including text, images, and videos- making their existence nearly undetectable. The web application will feature a user-friendly interface designed for seamless encryption, message hiding, and sharing. To enhance security, the project will incorporate multi-factor authentication, such as passwords and biometrics, along with Public Key Infrastructure (PKI) for secure exchange of messages. The initial scope excludes advanced features such as real-time messaging and extensive file-sharing capabilities. While multi-factor authentication and PKI will be included, other advanced security measures like end-to-end encryption will not be part of this project. The project aims to create a robust, secure, and user-friendly web application for covert communication, it will help improve our skills in web application development and cybersecurity.

8 Hardware/Software Tools and Cost

Table 1 represents the tools to develop the project.

Hardware Tools	
The project did not require Hardware tools.	
Software Tools	
Name and Description	Cost
 GitHub GitHub is a website and cloud-based service that helps developers store, manage and collaborate on their code.	Free
 Visual Studio Code Visual Studio Code is a versatile code editor that can run on different platforms and support various languages and frameworks.	Free



ChatGPT is an artificial intelligence tool that inspires us and is used to solve problems and differences in our ideas, as it also helps us think in new ways.

Free



Flask

Flask is a popular Python web framework that is widely used to design sophisticated web applications, APIs. As a result, this framework's simplicity, flexibility, scalability, reliability, and ability to process increased traffic are the key factors behind its popularity among businesses [1].

Free

 **Jira Software**

Jira is a software development tool for managing software development projects, enabling effective issue tracking and project management. It assists in planning, monitoring progress, and coordinating us to release our software project.

Free

9 Scrum Team

Skill Set Requirements

Table 2 Skill Set Requirements.

Technical Skill Required	What is the current level of the team (beginner-intermediate- advanced) for each skill? How will the gap be bridged? (if necessary) Learning plan
Programming using Python	Beginners, we can use our Java skills and watch tutorials or take Python courses to improve our performance.
cyber security skills	Intermediate
User Experience	Intermediate
Testing and debugging	Intermediate
Web-development skills	Advanced

Roles and Responsibilities

Scrum Team	
Product Owner: (list name of the student designated as a PO for the project)	Dr. Kholoud Al-Saleh
Developers: (list all student names)	Yara Alsubhi Arwa Mesloub Jana ALjomaih Khloud Aldoayan
Scrum Master (SM): (list name of designated SM for the project)	Dr. Kholoud Al-Saleh



كلية علوم الحاسب والمعلومات
قسم تقنية المعلومات

Stakeholders:

(list names of project stakeholders,
include customer names if any)

10 References

[1] Planecks , [planecks](#)