

Secure Steganography Web Application

Khadija Abdul Moiz¹, Adiba Unwaan², Sharanambe³, Akshata⁴, Ashok Bawge⁵

¹²³⁴⁵*Department of Computer Science and Engineering (IoT&Cybersecurity Including Blockchain Technology),*

Guru Nanak Dev Engineering College Bidar, Karnataka, India

Corresponding Author Email: khadija.moiz05@gmail.com

Abstract

In today's digital environment, keeping information secure and private is a major concern. Although encryption helps protect data, it can still reveal that sensitive communication is taking place. Steganography offers a different approach by hiding data inside ordinary media such as images, audio, or video, making it less noticeable. This project develops a web-based steganography application that combines encryption with data hiding to improve security. The message is first encrypted using AES or RSA and then embedded using techniques like LSB for images, frame-based methods for video, and phase coding for audio, ensuring minimal visible or audible changes. The system is built using Flask and Bootstrap, with libraries such as Pillow, OpenCV, Wave, and MoviePy for handling media files, and it runs without relying on cloud services to maintain privacy. Overall, the approach provides a practical and easy-to-use solution for secure communication, with uses in areas like confidential data sharing and digital content protection.

Keywords-Steganography, Cryptography, Data Hiding, LSB Technique, Multimedia Security, Web Application

1. Introduction

The rapid growth of digital communication has increased concerns regarding data security and privacy. While cryptography protects data by converting it into ciphertext, it does not hide the presence of communication, making it a potential target for attackers.

Steganography addresses this issue by embedding secret data within digital media such as images, audio, and video. When combined with cryptography, it provides dual-layer security by both encrypting the data and concealing its existence. Techniques such as Least Significant Bit (LSB), phase coding, and frame-based embedding enable efficient and imperceptible data hiding.

However, many existing systems are limited in functionality, often supporting only a single media type and lacking usability and flexibility.

To overcome these limitations, this paper presents a Secure Steganography Web Application that integrates multiple techniques with encryption in a unified and user-friendly platform. The system enables secure data embedding and extraction across

various media formats, providing a practical solution for secure communication.

2. Related Work

The increasing use of digital communication has created a strong need for secure data transmission. While cryptography protects the content of data, it does not hide its presence, which can attract unwanted attention. To address this, steganography is used to embed information within media such as images, audio, and video, making communication less noticeable [1]. Existing studies show that combining cryptography with steganography improves security by encrypting the data before embedding, reducing the chances of detection and unauthorized access [2].

Common steganographic techniques include Least Significant Bit (LSB) for images, phase coding for audio, and frame-based methods for video, each offering a balance between capacity and imperceptibility [3], [4]. LSB is widely used due to its simplicity, while phase coding provides better resistance in audio signals. Video-based methods further increase capacity by distributing data across frames.

However, many existing systems are limited, often supporting only a single media type and lacking proper usability and security features [5]. These limitations highlight the need for a more flexible and user-friendly system that integrates multiple techniques within a secure platform.

3. Materials and Methods

The methodology describes how the secure steganography web application was designed and implemented by combining cryptography, data hiding techniques, and web technologies. The system follows a client-server model, where users interact through a browser while a Flask-based backend handles processing. It allows secure login, embedding, and extraction of data across images, audio, and video files. Before embedding, the message is encrypted to improve security, and different techniques are used depending on the media type, such as LSB for images, phase coding for audio, and frame-based methods for video.

The application is built using Flask with supporting libraries like Pillow, OpenCV, MoviePy, and Wave for handling different media formats, along with standard encryption modules. The general workflow involves uploading a file, encrypting the message, embedding it into the media, and downloading the modified output, while extraction follows the reverse process.

The system is designed to be simple to use, efficient, and compatible across platforms, with minimal impact on media quality. Basic testing was carried out to check functionality, performance, and security, and the system was found to work reliably with different types of media.

4. Results and Discussion

The Secure Steganography Web Application was developed and tested using different types of media, including images, audio, and video. The system was able to successfully embed and retrieve hidden messages in all cases. Techniques such as LSB for images, phase coding for audio, and frame-based embedding for video worked as expected, with no noticeable change in the quality of the original files.

The encrypted messages remained secure, as extracted data could not be understood without the correct key. The time taken for embedding and

extraction was reasonable for small and medium-sized files, and the system handled different formats without major issues.

The login and access control features functioned properly, allowing only authorized users to use the system. Overall, the application performed reliably and met the goal of providing a simple and secure way to hide and retrieve information within digital media.

5. Conclusion

The Secure Steganography Web Application meets its goal of enabling secure communication by combining encryption with data hiding techniques. It allows users to embed secret information within images, audio, and video files in a way that does not noticeably affect the original media. Methods such as LSB, phase coding, and frame-based embedding were implemented and worked reliably during testing. The system was built using Flask along with supporting libraries for media processing, and includes a basic login feature to restrict access. It performed consistently across different file types and provided a simple interface for users to embed and extract data. Overall, the project shows that steganography can be applied in a practical web-based system for protecting sensitive information, and it can be further improved by adding advanced features such as stronger encryption, smarter detection resistance, or cloud support in the future.

References

- [1] G. C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner," 2016.
- [2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding—A Survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.
- [3] A. Cheddad, J. Condell, K. Curran, and P. McKeivitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [4] M. Hussain and M. Hussain, "A survey of image steganography techniques," *International Journal of Advanced Science and Technology*, vol. 54, pp. 113–124, 2013.
- [5] S. Baluja, "Hiding images in plain sight: Deep steganography," *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.
- [6] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis: A survey," *IEEE Signal Processing Magazine*, vol. 35, no. 3, pp. 27–41, 2018.
- [7] K. Muhammad, J. Ahmad, and S. W. Baik, "Secure data hiding in image using encryption and steganography," *IEEE Access*, vol. 7, pp. 144535–144549, 2019.

AdaptSec: A Gamified Cyber security Learning Application

Rajrajeshwari¹, Rishikesh Auradkar², Akash Ladde³, Shreyas⁴, Harish Joshi⁵

¹²³⁴⁵*Department of CSE (IoT & Cyber Security Including Blockchain Technology)*

Guru Nanak Dev Engineering College, Bidar, Karnataka, India

*Corresponding Author Email: rajeshwaridani97@email.com

Abstract

In today's highly connected digital environment, individuals face growing threats such as phishing, data breaches, and identity theft. However, many beginners struggle to learn cybersecurity because most training methods are too technical and difficult to understand. AdaptSec addresses this gap by providing a gamified and interactive platform that makes cybersecurity simple and engaging. The app focuses on practical learning through features like awareness surveys, password strength analysis, quizzes, and mini-games. It includes interactive games such as *Phish Shooter*, *PassForge*, and *NetShield*, which help users develop essential skills like identifying phishing attempts, creating secure passwords, and understanding basic network safety. Developed using HTML, CSS, and JavaScript, AdaptSec is lightweight, user-friendly, and accessible across devices. It integrates tools like *zxcvbn* for password evaluation and *jsPDF* for generating performance reports. With a modular and scalable design, the platform allows easy expansion with new features while maintaining a smooth and intuitive user experience.

1. Introduction

In today's digital era, cybersecurity has become essential due to the rapid growth of online activities such as digital banking, e-commerce, and social networking. This expansion has led to a significant rise in cyber threats, including phishing, data breaches, malware, and identity theft. However, many users still lack basic cybersecurity awareness because traditional learning methods are often complex and difficult to understand.

To address this issue, AdaptSec is developed as a gamified cybersecurity learning application that simplifies complex concepts through interactive and user-friendly methods. The platform uses surveys, quizzes, and real-time feedback along with engaging mini-games such as *Phish Shooter*, *PassForge*, and *NetShield* to help users understand and practice safe digital behavior.

Built using HTML, CSS, and JavaScript, AdaptSec ensures accessibility across devices without requiring installation. It integrates tools like *zxcvbn* for password strength analysis and *jsPDF* for report generation. By combining gamification with practical learning, AdaptSec effectively bridges the gap between theoretical knowledge and real-world cybersecurity practices, making it suitable for beginners and general users.

2. Related Work

Recent advancements in cybersecurity education highlight a shift from traditional theoretical methods to interactive and learner-centered approaches. Studies indicate that users understand and retain security concepts more effectively when learning is delivered through engaging and practical formats rather than static content. With the increasing prevalence of threats such as phishing, malware, and weak password practices, simplifying cybersecurity concepts for non-technical users has become essential.

Traditional awareness programs primarily focused on theoretical knowledge and general campaigns, which often lacked hands-on practice and real-world application. As a result, users frequently failed to apply learned concepts in practical scenarios. This limitation has led to the growing demand for interactive systems that provide simulations, immediate feedback, and experiential learning.

Gamification has emerged as an effective solution to improve user engagement and knowledge retention. Research shows that game-based learning enhances motivation and encourages users to repeatedly practice cybersecurity skills through challenges,

quizzes, and rewards. Such approaches not only increase participation but also promote long-term behavioral changes.

Additionally, web-based and modular learning platforms developed using technologies like HTML, CSS, and JavaScript have gained importance due to their accessibility and ease of use. Tools such as zxcvbn enable real-time password strength evaluation, while jsPDF supports performance tracking through report generation. Survey-based learning methods further enhance awareness by providing personalized insights into user behavior.

Overall, existing research emphasizes the need for integrated platforms that combine gamification, real-time feedback, and modular design. AdaptSec aligns with these findings by offering a comprehensive, user-friendly solution that improves cybersecurity awareness through interactive and practical learning.

3. Materials and Methods

The AdaptSec system is designed as a web-based cybersecurity learning platform developed using HTML, CSS, and JavaScript. The initial phase involved analyzing existing cybersecurity awareness tools and identifying their limitations. Based on this analysis, key requirements such as interactivity, gamification, accessibility, and real-time feedback were defined. A modular architecture was adopted to ensure scalability, flexibility, and ease of maintenance.

The system consists of multiple functional modules, including learning modules, gamification modules, password strength analysis, survey and analytics, report generation, and user interface components. Each module performs specific tasks and interacts with others through well-defined interfaces, enabling easy modification and future expansion.

AdaptSec integrates interactive learning methods such as tutorials, simulations, quizzes, and scenario-based exercises to enhance user understanding. Gamification elements like points, levels, and challenges are used to improve engagement and knowledge retention. The platform includes three main games—Phish Shooter, PassForge, and NetShield—which simulate real-world cybersecurity scenarios.

A password analysis module is implemented using the zxcvbn library to evaluate password strength in real time and provide improvement suggestions. Additionally, a survey-based risk assessment module collects user

responses related to online behavior and generates personalized feedback to identify potential security risks.

User performance is tracked through quiz scores, game results, and survey analysis. The jsPDF library is used to generate downloadable reports summarizing user progress, strengths, and areas for improvement.

The system operates entirely on the client side, ensuring easy accessibility without installation or server dependency. Testing was conducted at multiple levels, including unit testing, integration testing, and user acceptance testing, to ensure reliability and usability.

Overall, the proposed workflow includes user interaction with learning modules, participation in games and quizzes, system-based analysis of responses, and generation of personalized feedback and reports. This structured approach enhances cybersecurity awareness through practical and interactive learning.

4. Results and Discussion

The AdaptSec platform demonstrates effective performance through functional, visual, and analytical outputs, validating the efficiency of the proposed system. All modules, including surveys, games, quizzes, password analysis, and report generation, operate smoothly to provide an interactive learning experience.

Functionally, users can easily navigate through different modules such as the dashboard, survey, games, and quizzes. The system provides personalized feedback based on user behavior and classifies users into categories such as Safe, Moderate, and At Risk. Gamified modules like Phish Shooter, PassForge, and NetShield generate scores and feedback, helping users improve skills such as phishing detection, password creation, and network security. The quiz module offers randomized questions with instant evaluation, while the password analysis module uses zxcvbn to provide real-time strength assessment and improvement suggestions. Additionally, the system generates comprehensive PDF reports using jsPDF, summarizing user performance and recommendations.

From a visual perspective, the platform features a cyber-themed interface with responsive design, smooth animations, and graphical feedback elements such as progress bars and score indicators. These features enhance user engagement and improve usability across multiple devices.

Analytically, the system evaluates user performance by identifying strengths and weaknesses in cybersecurity practices. It detects common password vulnerabilities and analyzes user behavior through survey responses, providing meaningful insights for improvement.

Overall, the results indicate that the proposed system significantly enhances user engagement, learning outcomes, and cybersecurity awareness compared to traditional methods. The integration of gamification, real-time feedback, and modular design contributes to an effective and user-friendly learning platform.

5. Conclusion

This paper presents AdaptSec, a gamified cybersecurity learning application designed to make complex security concepts simple, interactive, and accessible for beginners and general users. By integrating games, quizzes, surveys, and real-time feedback, the system promotes practical learning and helps users develop essential skills such as phishing detection, password strengthening, and safe online behavior.

The platform's modular web-based architecture, developed using HTML, CSS, and JavaScript, ensures scalability, flexibility, and efficient performance. The use of tools such as xzcvbn and jsPDF further enhances functionality by enabling real-time password evaluation and automated report generation while maintaining user privacy.

Overall, AdaptSec demonstrates that gamification and interactive learning significantly improve user engagement, knowledge retention, and cybersecurity awareness compared to traditional methods. In the future, the system can be extended with features such as AI-based personalized learning, cloud integration, and advanced security simulations, making it a comprehensive solution for cybersecurity education.

References

- [1] Z. Yan et al., "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?," *Computers in Human Behavior*, vol. 84, pp. 375–382, 2018.
- [2] T. van Steen and J. R. Deeleman, "Successful gamification of cybersecurity training," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 593–598, 2021.
- [3] R. Matovu, J. C. Nwokeji, T. Holmes, and T. Rahman, "Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges," in *IEEE Frontiers in Education Conference (FIE)*, 2022, pp. 1–9.
- [4] M. Malone et al., "To gamify or not? On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1135–1141.
- [5] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on Internet usage and cybersecurity awareness in students," in *14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 223–228.
- [6] T. Sawik, "A linear model for optimal cybersecurity investment in Industry 4.0 supply chains," *International Journal of Production Research*, vol. 60, no. 4, pp. 1368–1385, 2022.
- [7] S. O'Connor et al., "SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security," *Information Sciences*, vol. 580, pp. 524–540, 2021.
- [8] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101827, 2020.
- [9] M. M. Yamin, B. Katt, and M. Nowostawski, "Serious games as a tool to model attack and defense scenarios for cyber-security exercises," *Computers & Security*, vol. 110, p. 102450, 2021.
- [10] A. Abd-Alrazaq et al., "The effectiveness and safety of serious games for improving cognitive abilities among elderly people with cognitive impairment," *JMIR Serious Games*, vol. 10, no. 1, p. e34592, 2022.
- [11] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, vol. 102, p. 102154, 2021.