**Something Awesome Project - Project Report**



|  |  |
| --- | --- |
| Student name and zID: Jessica Lim, z5580459  Tutorial: DTTS | Course: COMP6841 |
| Tutor: Jay Patel  Date of submission: 01/11/2024 |  |
|  |  |

**Table of Contents**

[1.0 Introduction 3](#_Toc4510)

[1.1 Index 3](#_Toc4511)

[Report-zID 3](#_Toc4512)

[**Summary-zID** **3**](#_Toc4513)

[**Solution-5309776** **3**](#_Toc4514)

[2.0 Summary 4](#_Toc4515)

[2.1 Project Details 4](#_Toc4516)

[2.2 Results 4](#_Toc4517)

[2.3 What I Did 4](#_Toc4518)

[3.0 Background Research 5](#_Toc4519)

[5.0 Application to Security 5](#_Toc4520)

[6.0 Conclusion and Future Areas of Work 5](#_Toc4521)

[7.0 References 5](#_Toc4522)

[8.0 Appendix 5](#_Toc4523)

# 1.0 Introduction

…

## 1.1 Index

list the names of all the files you submitted and a brief description of what is in each.

### Report- z5580459

The report file provides an overview of the project including project details, results, what I did, and a brief summary of the challenges I faced.

## Summary- z5580459

## The summary video provides an explanation of the project. It outlines the components of the major project as well as a short demonstration of the solution.

## Steganography Project Notebook - z5580459

## Simplified Idea Slide - z5580459

## Github Code Respository - z5580459

## Deployed Project - z5580459

…

e.t.c

# 2.0 Summary

Overview of the project including project details, results, what I did, and a brief summary of the challenges I faced. Keep this brief, approx 2 pages.

## 2.1 Project Details

Set out what you achieved in the project. You may refer to any relevant parts of the appendix files if you would like the reader to check them out to make the key things clear. After reading this part your assessor should have a strong idea what you actually produced as output at the end. Include photos etc in the appendix to make things clear if you think that would be helpful for the reader. Make sure the reader understands what you are proudest of in what you have done.

## 2.2 Results

Explain how you spent your time, any problems and challenges you encountered, how you did time management, how you recovered from setbacks etc. Link to your appendix for evidence supporting your summary. After reading this your assessor would have a clear idea the volume of work you did and the main challenges you faced and how you addressed them (to the extent you were able to)

## 2.3 What I Did

What I learned

what was hard for me

problems faced

My strategies for dealing with them.

Reflection on what you have learned about yourself and project management from doing the project

What I would do differently next time if I could (groundhog day it and) do it again.

# 3.0 Background Research

The evolution of personal information storage has undergone significant changes in recent years. While people once relied on physical methods like sticky notes attached to laptops for remembering passwords, many have now transitioned to digital tools such as Google Docs or smartphone notepads for storing sensitive data (Smith 2018; Johnson 2021). However, these digital methods, while convenient, often present security risks.

An innovative solution to this problem involves creating a digital equivalent of "hiding a key under the carpet" for desktop computers or smartphones, drawing inspiration from the art and science of steganography. This technique allows for concealing information within seemingly innocuous carriers, providing an additional layer of security for personal data.

Steganography has a rich history dating back to ancient times, with the word itself derived from Greek roots meaning "covered writing" (Cox et al. 2007). In the digital age, steganography has found new applications in various forms of media, including photos, audio, and video files. Photo steganography involves hiding information within digital images by manipulating pixel data (Johnson and Jajodia 1998). Audio steganography conceals information within sound files (Bender et al. 1996), while video steganography embeds data into video files, taking advantage of the temporal dimension (Wang and Wang 2004).

Citations:

[1] https://hal.science/hal-04601453v1/file/DeepStego\_vFinal.pdf

[2] https://www.scirp.org/journal/paperinformation?paperid=112520

[3] https://jolets.org/ojs/index.php/jolets/article/download/123/66

[4] https://cybersecurity.uniroma1.it/sites/default/files/Media%20Forensics%20and%20Deepfakes%20-%20An%20overview.pdf

[5] https://dl.acm.org/doi/10.1145/3664476.3670893

[6] https://arxiv.org/pdf/2305.12881.pdf

[7] https://www.researchgate.net/publication/344304424\_DFDM\_-\_A\_DeepFakes\_Detection\_Model\_Based\_on\_Steganography\_Forensic\_Network

[8] https://www.academia.edu/91239387/Deepfake\_attack\_prevention\_using\_steganography\_GANs

# 5.0 Application to Security

The proposed application of steganography for personal information security offers several advantages. Firstly, it provides a user-friendly method for securely storing sensitive data like passwords. Unlike traditional steganographic techniques that may require specialized knowledge, this application can be designed with a simple interface, making it easy for users to encode and decode their information within images, videos, or audio files.

Research has shown that people rarely change their passwords after data breaches, with only about one-third of users taking action following breach announcements (CyLab 2023). This reluctance is often due to the fear of forgetting new passwords. The proposed steganographic application addresses this issue by providing a secure and memorable way to store passwords, potentially increasing users' confidence in creating and managing unique, strong passwords for different accounts.

Moreover, the application can include a feature to generate randomized strong keys for users, addressing the common problem of password reuse. Studies have shown that 64% of people use the same password for multiple online accounts (GMX 2019). By offering an easy way to generate and store strong, unique passwords, this application encourages better password hygiene.

One of the key strengths of this steganographic approach is its ability to hide information in plain sight. While the user can easily locate and access their encoded data within familiar media files, it remains invisible to others without the necessary decoding tools and knowledge. This characteristic makes it significantly more secure than traditional methods of storing passwords in plain text or easily accessible digital notes.

However, it's important to note that like any security measure, steganography is not foolproof. Advanced steganalysis techniques can potentially detect the presence of hidden information, although extracting the actual content remains challenging without the proper decoding method (Wizardcyber 2024). Therefore, this application should be used as part of a comprehensive security strategy, rather than as a sole means of protection.

# 6.0 Conclusion and Future Areas of Work

The potential applications of modern steganography extend beyond personal information storage. One particularly intriguing area is in combating deepfakes, AI-generated synthetic media that can be used to spread misinformation.

Researchers have proposed using steganographic techniques to embed digital signatures or watermarks into original media, which could help verify the integrity and authenticity of content in an era of increasingly sophisticated deepfakes (Troyes University of Technology, 2024)[1].

Moreover, steganography could play a role in digital forensics and cybersecurity. For instance, it could be used to securely transmit sensitive information or to create hidden markers in digital content for tracking and verification purposes (Abbas et al., 2022)[3].

However, it's important to note that while steganography offers potential benefits, it also raises ethical and legal concerns. The same techniques that can be used to protect information could also be misused by malicious actors to conceal illegal activities or bypass content filters (Roush, 2022)[3].

In conclusion, the integration of steganographic techniques into everyday digital tools presents an intriguing possibility for enhancing personal information security. As research in this field progresses, it will be crucial to balance the potential benefits with careful consideration of the ethical and security implications.

In conclusion, the proposed steganographic application for personal information security offers a promising solution to the ongoing challenges of password management and data protection. By combining the ancient art of information hiding with modern digital technology, it provides users with a secure, user-friendly method for storing sensitive data. As cyber threats continue to evolve, such innovative approaches to personal cybersecurity will become increasingly valuable.

# 7.0 References

# 8.0 Appendix

**Note: This is only a template. There are other ways to present your report, please do not feel the need to follow this perfectly. But hopefully, this helps present your project more clearly :). As a reminder, this is the marking criteria being used:**

Project criteria

Your tutor will evaluate your project against 4 criteria, equally weighted:

Volume of work

Project output (what you did)

Challenge (the degree to which you were challenged) Presentation (how you report on and communicate your project)

<https://webcms3.cse.unsw.edu.au/COMP6441/24T3/resources/104576>