CS808 Computer Security Fundamentals Data Smuggling Coursework

Course Name	Computer Security Fundamentals
Course Code	CS808
Exam/Coursework	Data Smuggling using Steganography
Final Deadline	Wed 11th November, 9am
Weighting	20% of final course mark
Estimated Hours	20 hours per student
Individual or Group	Pairs, individual by approval with lecturer- students must email **by 9am Friday 23rd October to identify they wish to work individually** Students should self-define their pairs through the team self-selection activity on MyPlace under “Assessment” **by 9am Friday 23rd October**
Deadline for Live Presentation	To present “live” on zoom, student pairs must email the lecturer by 9am Tuesday 2nd November. A mutually agreeable time will be identified in advance of the final deadline.
Feedback Type	Written ☒ Oral e.g. pre-recorded video or zoom call ☐ Both ☐
Individual Feedback Format	Rubric criteria selected at performance level, plus per pair written feedback
Class wide Feedback Format	Pre-recorded video summary of most common limitations and guidance for improvement
Feedback Return	Within 3 working weeks from the submission per University policy (2/12/2020)
Marking Criteria	See marking criteria section
Relevant University Policies	It is your responsibility to familiarise yourself with the university policies below. The University policies on late submission of coursework and extension requests can be found here: Late Coursework Submission Policy Coursework Extension Policy

	The University take plagiarism (including self-plagiarism) seriously, please see the University guidelines on this here: Plagiarism Student Booklet

Table 1

Non-compliance Penalty

Any non-compliance with the instructions provided are subject to a 10% penalty.

Assessment Context

Your cyber security firm has just secured a contract with a financial company to explore concerns around data smuggling, where individuals who work for the company exfiltrate sensitive data. The company feels confident in their countermeasures for insiders smuggling data using cryptography, but they are concerned about the concept of steganography. Since many of the workers in their Glasgow office are technically competent, they believe it may be possible for a member of staff to write a program which hides data in images in such a way as to be undetectable by the human eye.

Your boss has asked yourself and your colleague to perform research into the feasibility of such a breach. The exercise is designed for pairs (2 students) to complete together, but can exceptionally be completed individually.

You should identify your pair using the team self-selection activity on MyPlace by the deadline shown in Table 1. Any who has **not allocated themselves** to a pair by this deadline will be **allocated** one at **random unless they e-mail the lecturer to indicate they wish to complete it individually by the deadline in Table 1** next to 'Individual or Group'. Note that no accommodation for increased workload will be made for students who elect to complete the project individually.

Assessment Tasks

This aim of this assessed coursework is to **research steganography** in the assessment **context** provided, **explore the feasibility of the scenario**, and **present** your **findings** to your boss and the company through a pre-recorded **presentation**.

Students may follow a programming or non-programming route. The programming route requires an implementation of LSB steganography to hide text strings. The non-programming route requires a research report covering the feasibility of steganography, and an exploration of mitigation techniques (steganalysis). Additionally, both routes require a 10 minute presentation.

Steganography Programming Route

The program you write should be able to complete the following tasks:

- Hiding a string within a 24-bit bitmap cover image using the least significant bit algorithm. The programme should ask the user to provide the string, and ensure there is sufficient capacity to hide the string.
- Extract a string from a bitmap containing a string which has previously been hidden using the same program

You should be able to compile the program and run it on CIS Windows 10 installations. It must be written in Python version 3.7

Constraints

When developing the program, you are required to comply with the following constraints:

- All cover images should be 24 bit .bmp format
- You should assume that a number of least significant bits will be required at the start of the cover image to hide the size of the payload.
- Note the first 54 bytes of an image file contains data about the image and should not be altered.

- The code should not make use of external python libraries to implement the program except for the Pillow library (Pillow Library) which provides the necessary functionality to work with images
- Code should be written completely from scratch by students i.e. you should not use code someone else has written
- The program you write will be tested on a CIS Windows installation, but for robustness it is advisable to test your work on different operating systems if possible.

Important Notes

It's important to remember that testing shows the presence of errors, not the absence thus it's best to test your code in as many ways as you can think of, and on different machines.

Note that it is often easier to determine understanding of if your code is well written (e.g. high cohesion, clearly commented, variables and methods sensibly named).

All files have header information at the start. For an image this includes information such as an estimate of the size, the height and width of the image. In a windows .bmp file this is 54 bytes (see Windows BMP Header Format for a breakdown). Depending on how you read in the image, you may need to skip this header before altering values.

It is expected you will have to identify ways of working with bytes and bits in Python, as well as working with images in Python using Pillow. This is part of the assessment, as you are tasked with exploring the feasibility. If this is something you are not comfortable with, you are advised to follow the non-programming route.

Presentation of the Results and Program

You are required to prepare a 10-minute video presentation which covers the following points:

- An overview of how steganography works, including a discussion of the LSB algorithm (approx.1 min)
- How feasible it would be to write such software and use it for data smuggling
- Coverage of key steps in the process through explanation and demonstration of the lightweight Python application
- Your recommendations to manage the risk of such a breach

Steganography Non-Programming Route

This route requires additional research in place of programming. This should be included in the submission as an executive summary of research on insider threats more generally as well as a presentation. The executive summary should address the following:

- A brief overview of the insider threat
- Argue whether or not the company should be concerned about insider threats
- Highlight key actions which should be considered to mitigate insider threats

ACM Referencing style should be used, see ACM Reference formatting Guide for details. The executive summary should exceed no more than 600 words (exclusive of document title, team name and references).

Presentation

You are required to prepare a 10-minute video presentation which covers the following points:

- An overview of how steganography works, including a discussion of the LSB algorithm (approx.1 min)
- How feasible it would be to write such software and use it for data smuggling
- Consideration of the wider impact of such a scenario, in particular a review of the risk of insider threat as it relates to data smuggling and how this may be addressed as a company
- Your recommendations to manage the risk of such a breach

No penalty will be applied if the length plus or minus 10% of 10 minutes. A penalty of 10% will be applied for submissions which are longer than 11 minutes.

Note that **each student must speak**.

Students can be innovative and creative within the given context. For example the presentation could be recorded with the individual speaking to camera, or as a voice over slides, or any other format you can think of. It can take time to produce the final mp4, as such you must ensure you do so sufficiently in advance of the deadline. No accommodation will be made for mismanagement of time.

Alternatively, to give a live presentation, you must notify the lecturer by the deadline in Table 1.

Submission

If completing the **programming** route, your **.py files** along with **instructions** on **running** your code should be compressed in **a .zip** file and **uploaded** to the submission slot on **MyPlace**. If completing the **non-programming** route, the **1 page executive summary** should be **uploaded** to the submission slot on **MyPlace**.

Your **video presentation file** should be uploaded directly to MyPlace using Planet e-Stream – see instructions on how to do this here: E-stream Coursework Upload Instructions One submission should be made per pair, by a nominated student. It is a joint responsibility to ensure both students are agree with what is submitted for assessment.

If working as a pair, you can also submit a workload report – see details in the 'Workload Report' section.

Workload Report

The aggregated and weighted coursework mark for the coursework may be adjusted proportionately to represent individual contributions to the work.

Adjustments based on individual contribution will be established using a single A4 page workload record. Pairs are required to agree a workload record which details each team member and their contributions and responsibilities for the steganography coursework. This should be submitted alongside the code or executive summary and presentation by the deadline in Table 1. If your pair is agreed both members of the team contributed sufficiently then you need not submit a workload report. If no workload report is submitted it will be assumed both individuals have contributed equally.

Screen Capture Tools

There are a number of screen capture software options. For example ActivePresenter Active Presenter software provides a free version which does not restrict the time you can record or apply a watermark. Feel free to use whichever software or technology you like so long as there is video and audio together in a single file such as .mp4. Zoom is also an option.

Marking Criteria

This coursework assessment is worth 20% of your final mark for the course and will be marked out of 20 using the following rubric.

Criteria	0 points	1 point	2 points	3 points	4 points	5 points
Context understanding and critique	No significant attempt	Extremely limited evidence of understanding of the context. It is likely there are many errors in understanding and reasoning.	Evidence of some understanding of the context. However, it is limited perhaps through several issues with the arguments and reasoning	Evidence of good understanding, but with definite room for improvement. Perhaps the arguments and reasoning could be stronger, and/or there are some errors in understanding	Evidence of very good understanding, but with a small room for improvement.	Evidence of deep understanding of the context through representing strong arguments and reasoning in relation to the context.
Understanding of Feasibility	No significant attempt	The implementation or feasibility argument is limited in demonstration of understanding. The majority could be improved, such as in the order or steps, or support for feasibility argument.	The implementation or feasibility argument is satisfactory, but could be improved in several areas. For example, it may be using an inappropriate approach for multiple steps, or feasibility argument has multiple flaws in understanding.	The implementation or feasibility argument is good, but could be substantially improved in perhaps one or two areas. For example, it may be using an inappropriate approach for one of the steps, or feasibility argument may be somewhat convoluted.	The implementation or feasibility argument is very good, perhaps one or two small areas where it could have been improved such as a step being more convoluted than necessary.	The implementation or feasibility argument is executed to a level which could not be bettered in this context. It demonstrates a depth of understanding and uses appropriate arguments and techniques.
Risk Mitigation Proposal	No significant attempt	The mitigation steps proposed are very limited, likely infeasible, and not well supported.	The mitigation steps proposed are limited. They are mostly inappropriate, and the feasibility is unlikely to be fully considered. Evidence is also likely to be limited, or not sufficiently strong.	The proposed mitigation steps are somewhat appropriate. There are likely to be one or two substantial areas for improvement. For example, the feasibility has not been properly considered or choice of evidence is not sufficiently strong.	The proposed mitigation steps are mostly appropriate, feasible, and well supported with suitable evidence. There are one or two small areas for improvement. E.g. a proposed mitigation technique could be better supported.	The proposed mitigation steps are clearly appropriate, feasible, and well supported with suitable evidence.

Criteria	0 points	1 point	2 points	3 points	4 points	5 points
Communication	No significant attempt	Content is very difficult to follow, and is unclear. Pace and articulation are likely to be unclear and not confident.	Content is mostly difficult to follow and unclear. Pace and articulation are likely to be unclear and not confident.	Content is presented well, but with definite room for improvement. Perhaps there are several small sections where the structure or pace and articulation could be improved.	Content is presented well, and it is mostly easy to follow. However, there are one or two small areas for improvement. Perhaps a particular paragraph is misplaced, or difficult to follow.	Content is presented very well and is structured in a way which makes it easy for the viewer to follow. Pace and articulation are clear and confident.