MA30279 Machine Learning 2 and MA50290 Applied Machine Learning
Assessed Coursework 2 2023–24

General instructions

Set: Thursday 23rd November 2023

Due: Friday 8th December 2023 at 19:00 on Moodle

Estimated time required: The expected time to complete this coursework is 10-15 hours in total (including the writing-up).

Value: This assignment is worth 60% of the total assessment for MA30279 (Machine Learning 2) / MA50290 (Applied Machine Learning). In the questions below, the notation **[marks]** indicates the marks available for each part out of a total of 60.

Grading: The coursework will be graded as follows: 60% content (mathematical and technical tools employed); 40% presentation (clarity of exposition and scientific rigour).

Submission: You are expected to upload your final report to Moodle as a single pdf document. The report cannot be longer than **6 pages** (including code snippets and possible figures). Handwritten solutions are not accepted.

Code snippets: For this assignment, you do not need to produce a fully working code, but only code snippets as specified in the report structure. The code snippet should be written in Python and PyTorch syntax and you are expected to exercise care in the definition of tensors and other possible parameters involved, including their dimensions. Minor typographic mistakes in names of functions and libraries will be tolerated.

Conditions: You should not discuss the details of your work with anyone else. The work which you hand in must be your own. You should be prepared to explain anything which you write to an examiner if asked to do so. In particular, if it is discovered that all or part of your code or your written work has been copied, both parties involved risk a severe penalty and might lose all their marks on the assignment.
You should refer to the lectures notes, lab sessions and any other material provided during the course to inform your strategy and write your report. You are not supposed to use any additional sources to complete this assignment. If you use any specific results which have been provided in class or part of a code from a lab session, you are expected to quote them clearly.

GenAI use: The use of Generative AI is not permitted (type A category).

Length: The maximum length for this assignment is **6 pages** (approximately 3000 words), including snippet codes and possible figures.

Support and advice: Contact the unit convenor via email (`tab73@bath.ac.uk`), or during office hours (Fridays at 11:15-12:05).

Feedback: You will receive feedback within a maximum of three semester weeks following the submission deadline. The feedback will consist of your marked work and an overall feedback document commenting on the assessment.

Late submission of coursework: If there are valid circumstances preventing you from meeting the deadline, your Director of Studies may grant you an extension to the specified submission date, if it is requested before the deadline. Forms to request an extension are available on SAMIS.

- If you submit a piece of work after the submission date, and no extension has been granted, the maximum mark possible will be the pass mark.
- If you submit work more than five working days after the submission date, you will normally receive a mark of 0 (zero), unless you have been granted an extension.

Academic integrity statement: Academic misconduct is defined by the University as "the use of unfair means in any examination or assessment procedure". This includes (but is not limited to) cheating, collusion, plagiarism, fabrication, or falsification. The University's Quality Assurance Code of Practice, QA53 Examination and Assessment Offences, sets out the consequences of committing an offence and the penalties that might be applied.

Goal of the coursework

For this coursework you are asked to devise, and explain in a report of (maximum) 6 pages, a suitable deep learning strategy for a given concrete problem.

The goal of this coursework is **not** to get THE correct strategy (there are many plausible ones), but rather to show your critical thinking in deploying deep learning in a practical scenario, that is, how you apply what you learned **from this course** in a hypothetical, yet concrete situation.

Presentation of the problem

The company you are working for proposes digital solutions to conceal a message A in the form of an image inside another image B. This means that the image B acts as a 'hiding medium' to conceal A and, once A is concealed inside B, the resulting image C should be almost visually indistinguishable from B.

The image C is then sent to a third party who has access to an oracle which, given your concealing procedure, provides the most accurate *unveiling* operation D for that concealing procedure. The third party is then able to find an unveiled image U by applying the unveiling operation D as follows:

$$U = D(C). \tag{1}$$

Here, D is intentionally left unspecified because clearly the unveiling operation D depends on how the image C is generated (i.e. on the concealing procedure, which will be your task!). You can assume that you have access to the oracle that produces a well defined unveiling procedure D for a given concealing procedure. Note that you are not required to specify D for the concealing procedure you design.

Your task: Devise, and explain in the report, a deep learning strategy that, given images A and B, produces the image C that conceals A. In particular, you should consider and address the following points (see also the outline structure of the report detailed below): 1. mathematical introduction to the problem; 2. data handling; 3. deep learning model; 4. training of the deep learning model; 5. assessment of the results. You do **not** need to produce a fully working code, but only core parts of the code as specified in the report structure below. You can include additional lines of code in other sections of the report if you think it is necessary to explain your strategy, but be mindful that this counts towards the page limit.

Note: Your task does **not** involve designing the unveiling operation D. However, since the design of the concealing operation (i.e., your task for this coursework) affects what the third party has at its disposal to unveil the image (i.e., the unveiling operation D), you can speculate on D if this helps you devising your concealing strategy.

Report outline: Structure and content

The report must include the following sections and address all the points specified below.

1. **Introduction:** Provide a mathematical context for the problem. In particular:

(a) Specify in mathematical terms the desired criteria for this problem (e.g., how do you express in mathematical terms that "the resulting image C should look almost visually indistinguishable from B"?). **[3]**

(b) Do you think deep learning is suitable in this context? Explain why or why not. **[2]**

2. **Data handling:** Explain how you can prepare and handle data for this problem. In particular:

   (a) Explain what are your input datapoints and your output data. Specify the dimensions and if there should be any specific limitations to the size of the images involved. **[5]**

   (b) Explain how you organise the datapoints in suitable datasets for training, validation and testing. **[5]**

3. **Model:** Devise a suitable model for the concealing operation. In particular:

   (a) Describe a suitable deep learning architecture (choosing between a feed-forward neural network and a convolution neural network), explaining why you chose it and why it is suitable for this application. **[5]**

   (b) Specify width and depth of the network, activation function(s), and all the other necessary details to practically implement your network (e.g., if you chose a fully connected NN you should specify width and depth of the NN, or if you chose a CNN you should specify the filter size, stride and padding). Explain what considerations informed your strategy while designing your network. **[5]**

   (c) Provide a Python code snippet for the PyTorch class implementing the forward method of the neural network you devised. **[8]**

4. **Training:** Devise a suitable training procedure. In particular:

   (a) Specify the loss (and cost) function and the learnable parameters, explaining why you chose this loss (for example, why do you expect to work well for this problem?) and which favourable mathematical properties it has. **[5]**

   (b) Specify which optimisation algorithm you will use for the training phase, choosing among the algorithms covered during the course, and explain why it is amenable to the loss function you devised. Discuss parameter choices related to the algorithm of your choice (e.g., how do you select the learning rate and how do you initialise the learnable parameters). **[5]**

   (c) In addressing the above points, consider the various challenges training poses and discuss if any of the possible solutions we covered in the course (e.g., regularisation, early stopping, data augmentation) would be sensible and/or necessary within the deep learning strategy you are devising. **[5]**

   (d) Provide a Python code snippet implementing the loop over epochs for training your network using PyTorch. This should include the call to the cost function, back-propagation, and optimiser operations. There is no need to include code for printing or plotting results. **[7]**

5. **Assessment of results:** Explain how you will evaluate the correct functioning of your strategy. In particular:

   (a) Explain when you can consider the testing phase satisfactory. **[2]**

   (b) Discuss which quality metrics you would use in view of the learning strategy you devised. **[3]**