Introduction to AI Coursework

1 Anlysis on the Penguin Dataset

1.1 EDA on Penguin Datasets

This dataset comprimises features such as species, island and bill_length_mm. Firstly, I conducted an analysis to determine the type, number of values, number of unique values, and proportion of missing values for each feature within the dataset. The anlysis is present in Table 1.

Table 1: Summary of Features

Feature	Type	Count	Nunique	% Null
species	object	344	3	0.000000
island	object	344	3	0.000000
bill_length_mm	float64	342	164	0.581395
bill_depth_mm	float64	342	80	0.581395
flipper_length_mm	float64	342	55	0.581395
body_mass_g	float64	342	94	0.581395
sex	object	333	2	3.197674
year	int64	344	3	0.000000

Obviously, the proportion of missing values is not substantial. Therefore, rows containing missing values will be dropped. The distribution of numerical features is illustrated in Figure 1.
Subsequently, I employed Cramér's V statistic to measure the correlation between different features and generated a heatmap accordingly. According to Figure 1, the features sex and year exhibit the quite low correlation with species; hence, these two features will not be applied to build the prediction model.

1.2 Model Training

Before building the model, I preprocessed the data based on the previous analysis. Firstly, I dropped the features sex and year. Then, I utilised label encoding to encode the categorical feature island and the target feature

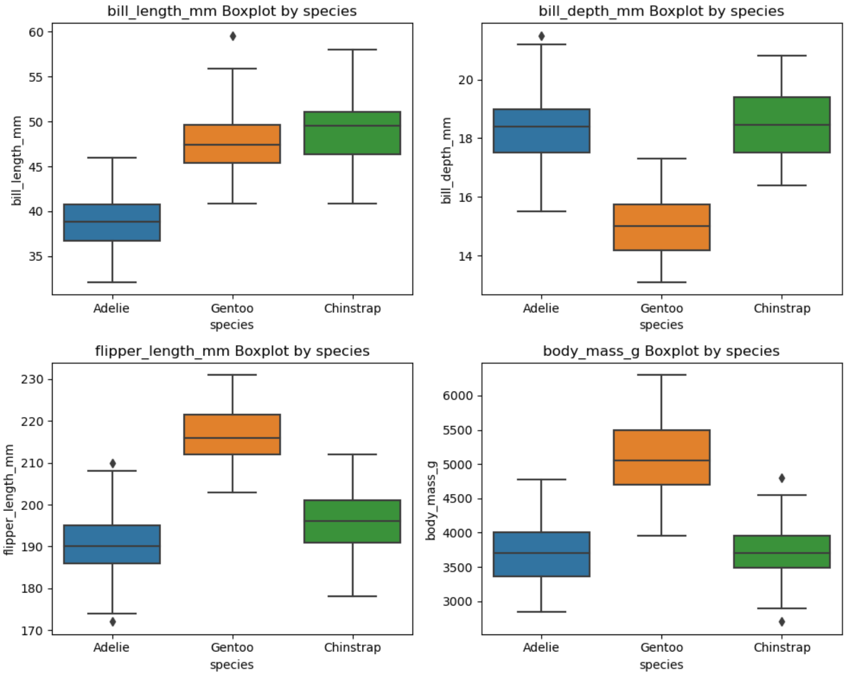
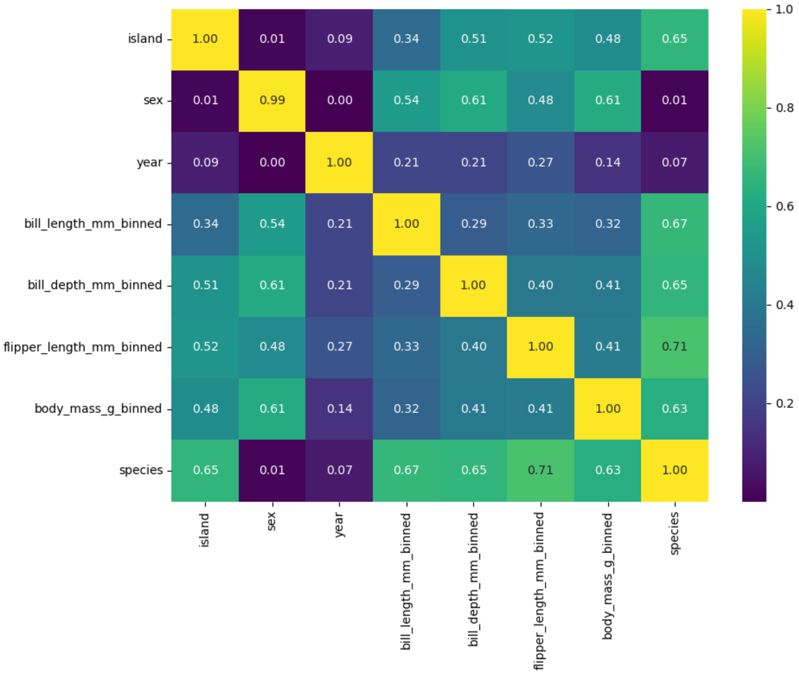


Figure 1: Distribution of different numerical features



	island	sex	year	bill_length_mm_binned	bill_depth_mm_binned	flipper_length_mm_binned	body_mass_g_binned	species
island	1.00	0.01	0.09	0.34	0.51	0.52	0.48	0.65
sex	0.01	0.99	0.00	0.54	0.61	0.48	0.61	0.01
year	0.09	0.00	1.00	0.21	0.21	0.27	0.14	0.07
bill_length_mm_binned	0.34	0.54	0.21	1.00	0.29	0.33	0.32	0.67
bill_depth_mm_binned	0.51	0.61	0.21	0.29	1.00	0.40	0.41	0.65
flipper_length_mm_binned	0.52	0.48	0.27	0.33	0.40	1.00	0.41	0.71
body_mass_g_binned	0.48	0.61	0.14	0.32	0.41	0.41	1.00	0.63
species	0.65	0.01	0.07	0.67	0.65	0.71	0.63	1.00

Figure 2: Correlation between different features

species. Finally, I split the dataset into training and testing sets according to a 4:1 ratio.

Table 2: Best parameters of Decision Tree and Random Forest

	Decision Tree	Random Forest
criterion	entropy	gini
max_depth	13	12
min_samples_split	13	17
min_samples_leaf	1	1
max_leaf_nodes	32	31
n_estimators	-	131

Criterion represents the criterion for node splitting, max_depth is the maximum depth of the decision tree, min_samples_split is the minimum number of samples required to split a node, min_samples_leaf is the minimum number of samples required to be at a leaf node. max_leaf_nodes is the maximum number of leaf nodes, and n_estimators is the number of decision tress.
The KNN was employed as the baseline model because KNN is a non-parametric and lazy method, meaning that the model does not explicitly learn from the data during the training phase. Moreover, I also applied Decision Tree and Random Forest algorithms to build two classification models. In this research, optuna was employed for fine-tuning. The monitoring metric for parameter tuning is the average accuracy obtained through 5-fold cross-validation. The optimal parameters are determined by the highest average accuracy achieved across 50 trials.

1.3 Results Evaluation

In this research, the confusion matrix was utilised to evaluate the performance of different models.

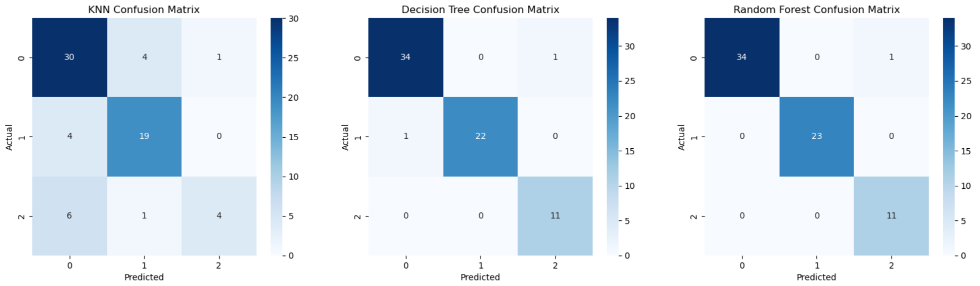


Figure 3: Confusion Matrix

As shown in Figure 2, both the decision tree and random forest models exhibit higher classification performance compared to KNN. The random forest model has only one misclassification, while the decision tree has two misclassifications, and KNN has 20 misclassifications.

Table 3: Models' performance on different metrics

-	KNN	Decision Tree	Random Forest
accuracy	0.77	0.97	0.99
macro avg precision	0.78	0.96	0.97
macro avg recall	0.68	0.98	0.99
macro avg f1-score	0.70	0.97	0.98

In addition, accuracy, macro average precision, macro average recall, and macro average F1-score were employed to evaluate the performance of the models. As shown in Table 3, he performance of both the decision tree and random forest models surpassed the baseline model KNN across all metrics. Among them, the random forest model exhibited the best classification performance, achieving the highest scores across all metrics.

2 Challenges in AI

The advancement of AI technology is gradually reshaping human society. Both the personalised recommendations on video platforms like YouTube and the drones employed to execute perilous tasks by are outcomes of AI algorithm applications. Undeniably, AI technology has brought us many conveniences. However, the application of AI technology also brings forth numerous issues and challenges. As a data-driven technology, undoubtedly, this raises concerns regarding data protection.

In the 2010s, the Facebook–Cambridge Analytica data scandal that occurred drew widespread public attention. Cambridge Analytica utilised user data to target political advertisements without obtaining consent from the users. Finally, Facebook was fined \$5 billion for this incident. In this incident, the role of the law was primarily punitive after the fact. Indeed, proactive constraints are equally important. Many countries and regions around the world have made efforts in this regard, such as the European Union's GDPR. Additionally, companies should fulfill their ethical obligations to ensure that users have the right to be informed about and to decide on the usage of their data.

The security of AI is also a topic of ongoing public concern. In 2019, a Tesla car owner was charged with manslaughter for a fatal traffic accident involving the use of the semi-autonomous driving system Autopilot. Aside from personal safety, AI also has the potential to impact social order. The recent popularity of generative AI also poses the risk of being abused. For exam-

ple, in 2023, A fake news video featuring a fabricated speech by Japanese Prime Minister Fumio Kishida, created by an internet user, went viral online, garnering millions of views in a short period. To address the potential risks associated with AI, the European Union introduced the Artificial Intelligence Act in 2023 to tackle these challenges. According to the AI Act, artificial intelligence systems will be categorized into four different risk levels. For high-risk artificial intelligence systems, the "Artificial Intelligence Act" establishes a comprehensive lifecycle regulatory framework covering pre-market, in-market, and post-market stages. The implementation of differentiated regulation for artificial intelligence systems based on different risk levels provides a potential solution. developers of AI should also uphold the most fundamental social responsibility. Moreover, efforts should be made to enhance the robustness and reliability of AI systems, thereby minimizing the risks associated with AI technology as much as possible.
In conclusion, to address the challenges posed by AI, it is crucial to enhance legal frameworks, as laws serve as the most robust safeguard for societal order. In addition to legal frameworks, Furthermore, AI developers should establish reliable accountability mechanisms to prevent the misuse of data and mitigate the adverse effects of AI systems.

References

[1] Leslie Lamport, *LaTeX: a document preparation system*, Addison Wesley, Massachusetts, 2nd edition, 1994.

[2] Wikibooks, *LaTeX/Bibliography Management*, [0nline], Accessed at https://en.wikibooks.org/wiki/LaTeX/Bibliography_Management, (DATE ACCESSED).