FORGED BANK NOTE PREDICTION

Saleem Thapa

Fall 2023

Contents

List of Figures

1 Introduction

This project is dedicated to the exploration of banknote authentication through machine learning with a specific emphasis on neural network architectures implemented using TensorFlow. The primary objective is to develop a biased model proficient in distinguishing genuine banknotes from counterfeit ones based on features such as variance, skewness, curtosis, and entropy. The project adopts a systematic approach, commencing with a logistic regression model and progressively expanding the complexity of neural network structures to ascertain the point of overfitting the entire dataset.

A fundamental aspect of this investigation is the meticulous determination of the requisite neural network size, informed by an iterative experimentation process. Notably, the endeavor eschews the utilization of pre-existing libraries to foster an intricate comprehension of the neural network's underlying mechanisms and facilitate strategic decision-making regarding model architecture. This iterative exploration aims to yield insights into feature importance, model performance metrics, and potential strategies for feature reduction.

2 Dataset

The dataset was obtained from the UCI Machine Learning Repository. The dataset,banknote-authentication.csv, for the classification problem contains a total of 1372 instances (rows) and consists of 5 variables (columns). The variables employed as inputs for the classification task encompass the variance, skewness, and curtosis of the wavelet-transformed data, the entropy of the image, along with the class which defines whether the note is Forged or Real.

2.1 Visualization of the distribution of each feature

The histogram plot and scatter plot of every input features showing their maximum and minimum value as well as how they are distributed can be seen in the images given below.

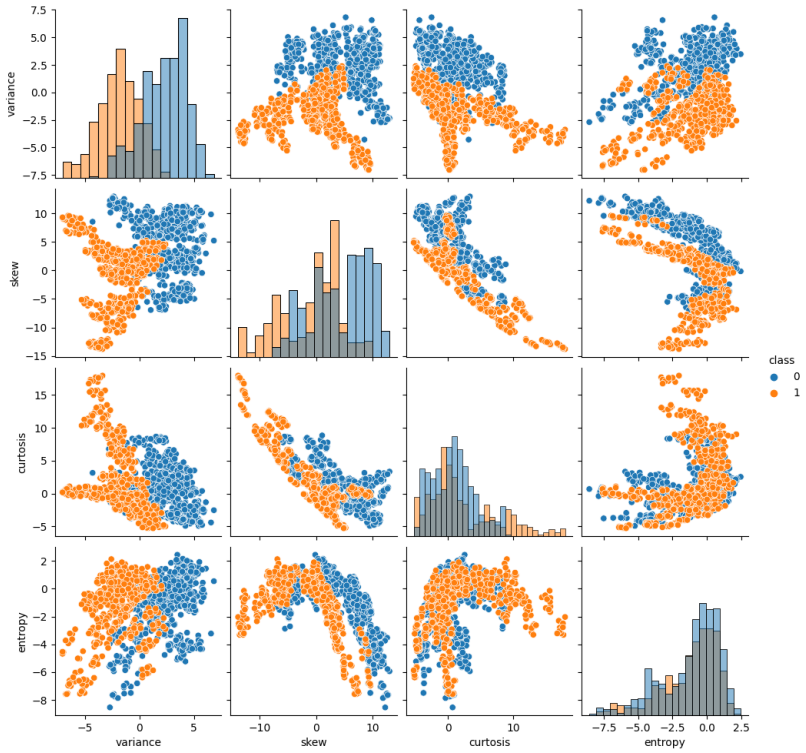

Figure 1: Different input features

	Min	Max	Mean	Std
Variance	-7.0421	6.8248	0.433735	2.842763
Skew	-13.7731	12.9516	1.922353	5.869047
Cutosis	-5.2861	17.9274	1.397627	4.310030
Entropy	-8.5482	2.4495	-1.191657	2.101013
Class	0.0000	1.0000	0.444606	0.497103

Table 1: Input Feature Statistics

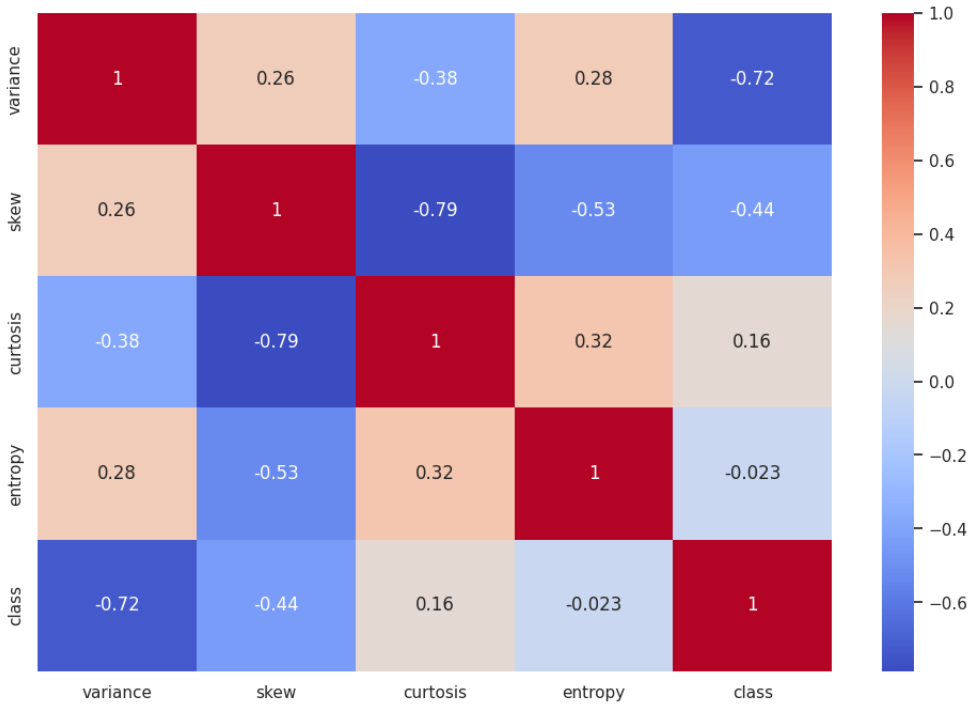

Figure 2: Correation Matrix Heatmap

3 Data Processing

3.1 Data spliting

Dataset was splitted into Training , Validation and Testing where 80 percent of the data was allocated for training , 10 percent for Validation and Rest 10 percent for Testing.

3.2 Data Normalization

In the preprocessing steps, we applied two distinct normalization techniques to the input features of our dataset, aiming to enhance the performance and convergence of our neural network model. The first normalization method employed was Min-Max normalization, which involves scaling the features to a specific range, typically between 0 and 1. To achieve this, we calculated the minimum and maximum values for each feature across the entire dataset and then transformed the features based on the formula (value - min) / (max - min). This ensures that all features share a consistent scale, promoting stable and effective learning during the model training process.

Following Min-Max normalization, we implemented Z-score normalization, also known as standardization. This technique involves transforming the features to have a mean of 0 and a standard deviation of 1. To achieve this, we computed the mean and standard deviation for each feature across the dataset and then applied the transformation using the formula (value - mean) / standard deviation. Z-score normalization is particularly useful when dealing with datasets that may contain outliers, as it is less sensitive to extreme values. By performing both Min-Max and Z-score normalization, we aimed to provide our neural network with standardized input features, contributing to improved training stability and convergence.

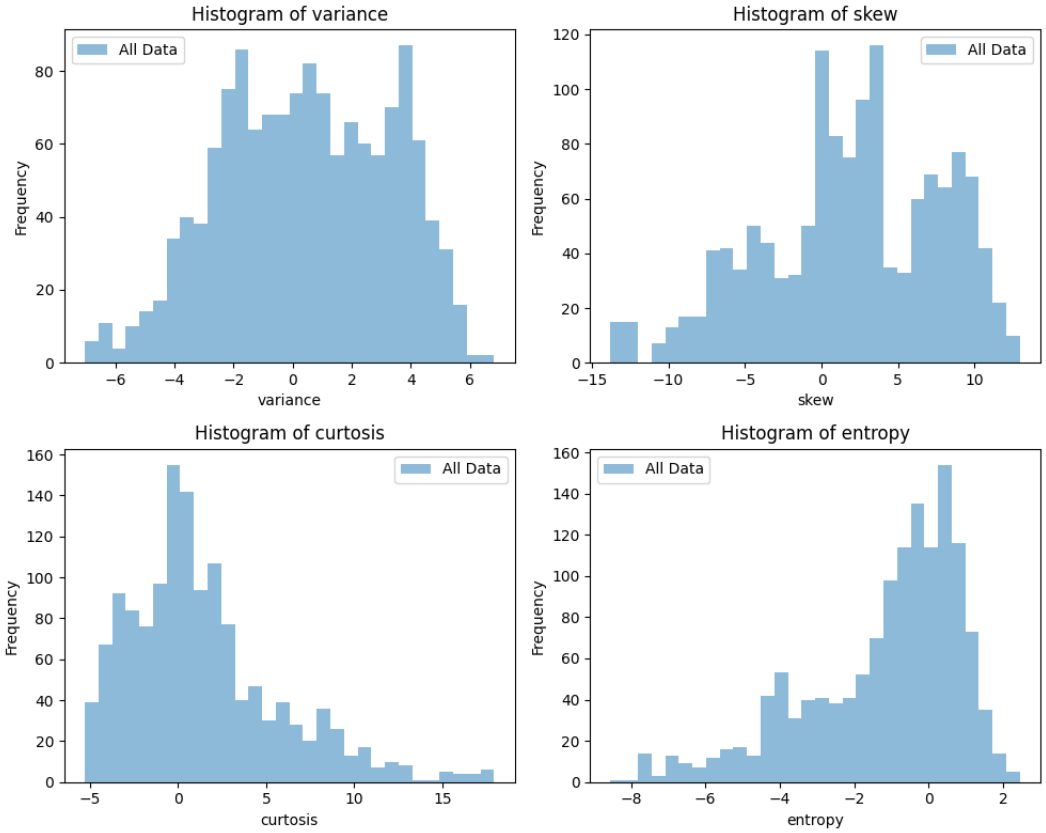

Figure 3: Data Before Normalization

4 Modeling

In constructing our neural network model, we utilized the TensorFlow and Keras frameworks to design and train a custom architecture tailored for binary classification. The input layer of the model corresponds to the number of features in our dataset, and we incorporated three hidden layers, each with a Rectified Linear Unit (ReLU) activation function to introduce non-linearity to the model. The final output layer employed a sigmoid activation function, suitable for binary classification tasks.

The model was compiled using the binary cross-entropy loss function, which measures the dissimilarity between predicted and actual class labels, and we employed stochastic gradient descent (SGD) as the optimizer to iteratively adjust the model's parameters. To prevent overfitting, we implemented early stopping during training, monitoring the validation loss and terminating the training process if no improvement was observed within a predefined patience period.

Throughout training, we monitored the loss at regular intervals and printed updates to assess the model's convergence. Furthermore, we calculated the training accuracy by comparing the model's predictions on the training set with the actual labels. This information provided insights into the model's performance during each training epoch. Finally, after the training process, we evaluated the model's accuracy on a validation set to gauge its generalization performance on unseen data. This approach allowed us to iteratively refine the model architecture and training parameters, ultimately achieving a well-generalized neural network for the binary classification task.

5 Model Selection

The provided output indicates the performance of different neural network architectures on the training and validation sets. Here's an explanation for each model architecture:
Model Architecture: [16, 8]
Accuracy on Training Set: 100.00%
Accuracy on Validation Set: 100.00%
This architecture with two hidden layers of 16 and 8 neurons, respectively, achieved perfect accuracy on both the training and validation sets. While achieving 100% accuracy on the training set may suggest overfitting, the model generalized well to the validation set, indicating effective learning.

Model Architecture: [8, 1]
Accuracy on Training Set: 55.97%
Accuracy on Validation Set: 53.82%
This architecture, with one hidden layer of 8 neurons, demonstrated lower accuracy on both the training and validation sets. The lower accuracy suggests that the model complexity might not be sufficient to capture the underlying patterns in the data, leading to a less effective classifier.

Model Architecture: [4, 1]
Accuracy on Training Set: 99.91%
Accuracy on Validation Set: 99.64%
This architecture, with one hidden layer of 4 neurons, achieved high accuracy on both the training and validation sets. The model demonstrated strong performance and generalization, but it may be slightly overfitting as the accuracy on the training set is very close to 100%.

Model Architecture: [2, 1]
Accuracy on Training Set: 100.00%
Accuracy on Validation Set: 100.00%
This architecture, with one hidden layer of 2 neurons, achieved perfect accuracy on both the training and validation sets. Similar to the first model, it raises a potential concern of overfitting, but it also indicates that the model learned to

classify the data effectively.

In summary, the models with more neurons in the hidden layers ([16, 8] and [2, 1]) achieved perfect accuracy, while the simpler models ([8, 1] and [4, 1]) showed slightly lower accuracy. Further analysis, such as examining learning curves and considering metrics like precision, recall, and F1 score, would provide a more comprehensive understanding of model performance and help in selecting the best model.

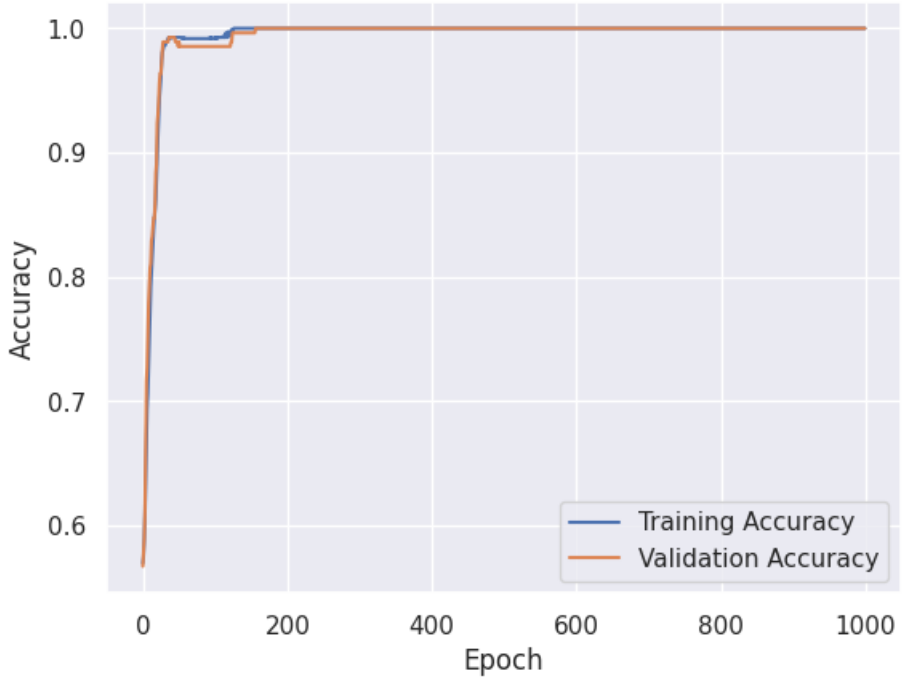

Figure 4: Learning curve for the best model

6 Model Evaluation

In the evaluation of our fraud note detection model, we employed various performance metrics to gauge its effectiveness. With a threshold of 0.32, our model achieved an accuracy of 54.01%, signifying the overall correctness of predictions. However, in fraud detection scenarios, accuracy alone might not provide a comprehensive understanding of a model's performance due to the class imbalance present.

Delving into more nuanced metrics, the precision of 47.54% reveals the pro-

portion of predicted counterfeit notes that are truly fraudulent. This is an essential metric in financial fraud detection, as it sheds light on the reliability of our model when identifying potentially malicious instances. Concurrently, a recall of 48.33% highlights the model's ability to capture genuine fraudulent notes, emphasizing its sensitivity to such instances.

The F1 score, which harmonizes precision and recall, was calculated at 47.93%. This metric serves as a consolidated measure, considering both false positives and false negatives. Given the nature of fraud detection, striking a balance between precision and recall is crucial. A higher recall, in particular, is often prioritized in this context to minimize the risk of missing potentially fraudulent notes.

As we fine-tune our model and explore different threshold values, it is imperative to consider the implications of false positives and false negatives.

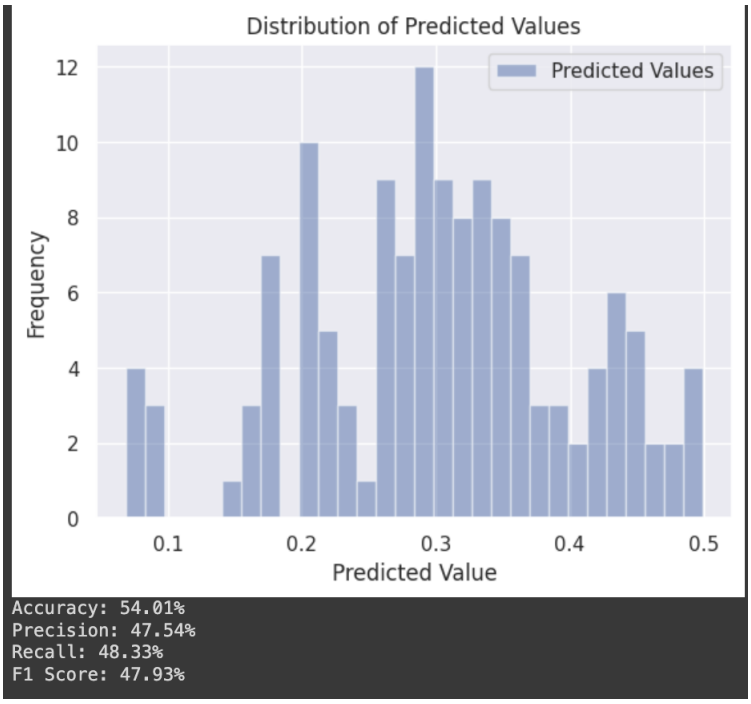

Figure 5: Model evaluation

Threshold	**Accuracy**	**Precision**	**Recall**	**F1 score**
0.5(default)	56.20%	100.00%	0.00%	0.00%
0.7	56.20%	100.00%	0.00%	0.00%
0.4	61.31%	64.00%	26.67%	37.65%
0.32	54.01%	47.4%	48.33%	47.93%

Table 2: Model Evaluation with different threshold values

The selection of the threshold value is crucial as it directly influences the trade-off between precision and recall. In our context of fraud note detection, where the consequences of both false positives and false negatives are impactful, a balanced approach is often preferred. A threshold of 0.32 appears to strike a reasonable balance between precision and recall.

With a threshold of 0.32, our model achieves a precision of 47.4% and a recall of 48.33%. This indicates that, when the model flags a note as fraudulent, it is accurate approximately 47.4% of the time, and it successfully captures around 48.33% of the actual fraudulent notes. The F1 score, a metric that considers both precision and recall, is 47.93%, suggesting a harmonious compromise.

In fraud detection scenarios, we aim to minimize both false positives (misclassifying genuine notes as fraudulent) and false negatives (missing actual fraudulent notes). The 0.32 threshold seems to offer a reasonable balance, acknowledging the inherent trade-offs and aiming for a model that provides a satisfactory level of accuracy while being sensitive to the identification of true fraudulent instances.

6.1 Learning Curve of Model using Sigmoid Activation

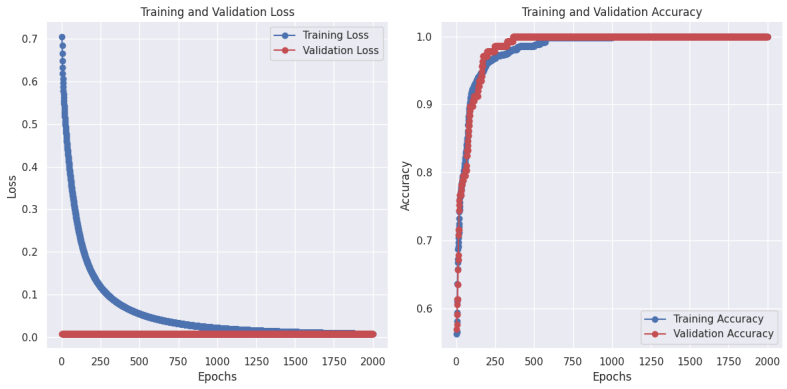

Figure 6: Curve showing change in loss vs accuracy

7 Feature Importance and Reduction

7.1 Performance of each feature

7.1.1 Variance vs Class

The dataset comprises 1,372 observations, primarily focused on the 'variance' feature, which exhibits a diverse range with a mean of 0.43 and a standard deviation of 2.84. The binary 'class' label, indicating authenticity (0) or fraudulence (1) of banknotes, shows a slight imbalance, with a mean of 0.44. The dataset's central tendency is moderate, and key percentiles, including the median at 0.50, provide insights into the distribution of 'variance.'

Notably, the presence of potential outliers, with a minimum of -7.04 and a maximum of 6.82, demands attention. While statistical measures offer a foundational understanding, further exploration through visualization and machine learning modeling is necessary for a comprehensive analysis of the 'variance' feature's performance in predicting banknote authenticity.

```
Feature Statistics:
          variance        class
count  1372.000000  1372.000000
mean      0.433735     0.444606
std       2.842763     0.497103
min      -7.042100     0.000000
25%      -1.773000     0.000000
50%       0.496180     0.000000
75%       2.821475     1.000000
max       6.824800     1.000000
```

Figure 7: Performance of variance feature

7.1.2 Skew vs Class

The dataset presents 1,372 observations, emphasizing the 'skew' feature, characterized by a mean of 1.92 and a standard deviation of 5.87. The binary 'class' label, denoting banknote authenticity (0) or fraudulence (1), displays a mean of 0.44, indicating a somewhat imbalanced distribution. Key percentiles provide further insights into the distribution of 'skew,' with the median at 2.32. A notable range of values is evident, ranging from a minimum of -13.77 to a maximum of 12.95, suggesting potential outliers. This statistical overview sets the stage for a comprehensive exploration of the 'skew' feature's performance, including visualization and machine learning modeling, to ascertain its role in predicting banknote authenticity.

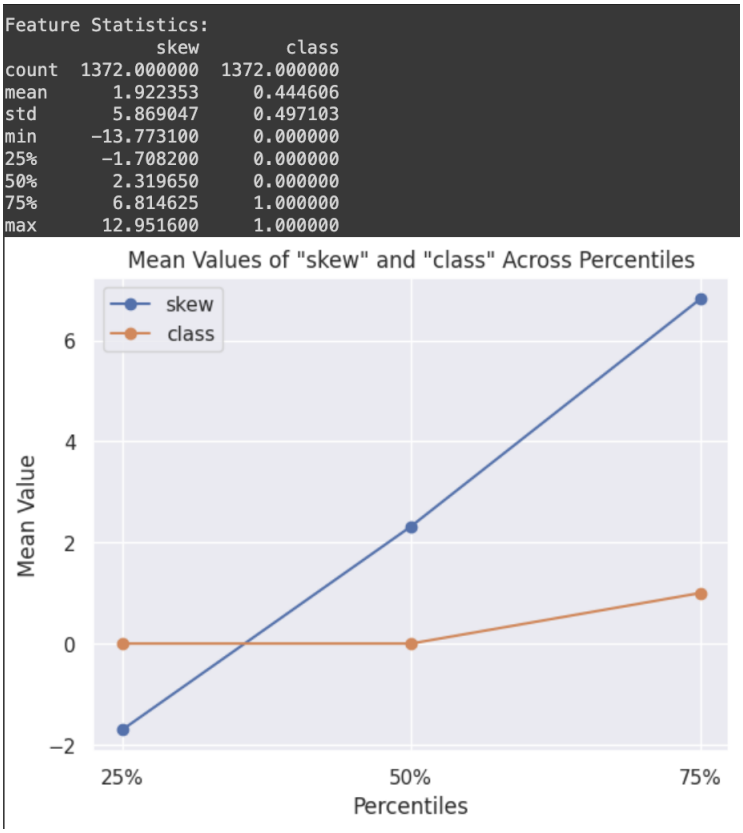

Figure 8: Performance of variance feature

7.1.3 Curtosis vs Class

The dataset includes 1,372 instances with a focus on the 'curtosis' feature, exhibiting a mean of 1.40 and a standard deviation of 4.31. The binary 'class' label indicating banknote authenticity (0) or fraudulence (1) shows a mean of 0.44, suggesting a slightly imbalanced distribution. Key percentiles reveal insights into the 'curtosis' distribution, with the median at 0.62. The feature spans a range from a minimum of -5.29 to a maximum of 17.93, highlighting potential outliers. Further exploration, including visualization and machine learning modeling, will be crucial to understanding the predictive power of 'curtosis' in distinguishing between genuine and counterfeit banknotes.

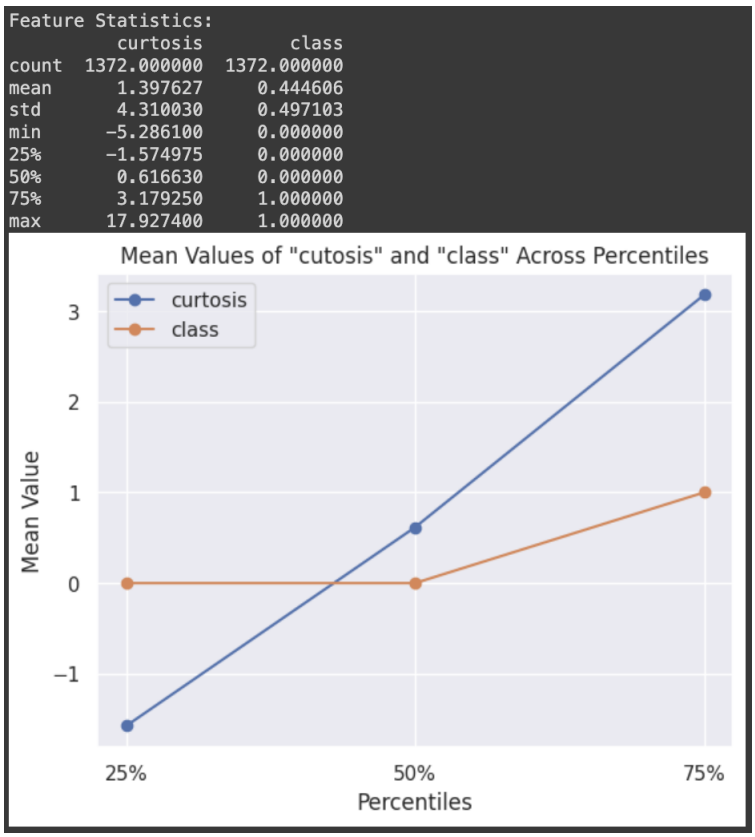

Figure 9: Performance of variance feature

7.1.4 Entropy vs Class

The dataset comprises 1,372 instances with a focus on the 'entropy' feature. The mean entropy is approximately -1.19, indicating a tendency towards lower

entropy values. The binary 'class' label, representing banknote authenticity (0) or fraudulence (1), has a mean of 0.44, suggesting a slightly imbalanced distribution. The 'entropy' feature exhibits a standard deviation of 2.10, with percentiles providing additional insights. The median is around -0.59, and the range spans from a minimum of -8.55 to a maximum of 2.45. These statistics lay the groundwork for understanding the distribution and characteristics of the 'entropy' feature, which will be further explored through visualization and modeling to assess its significance in differentiating between genuine and counterfeit banknotes.

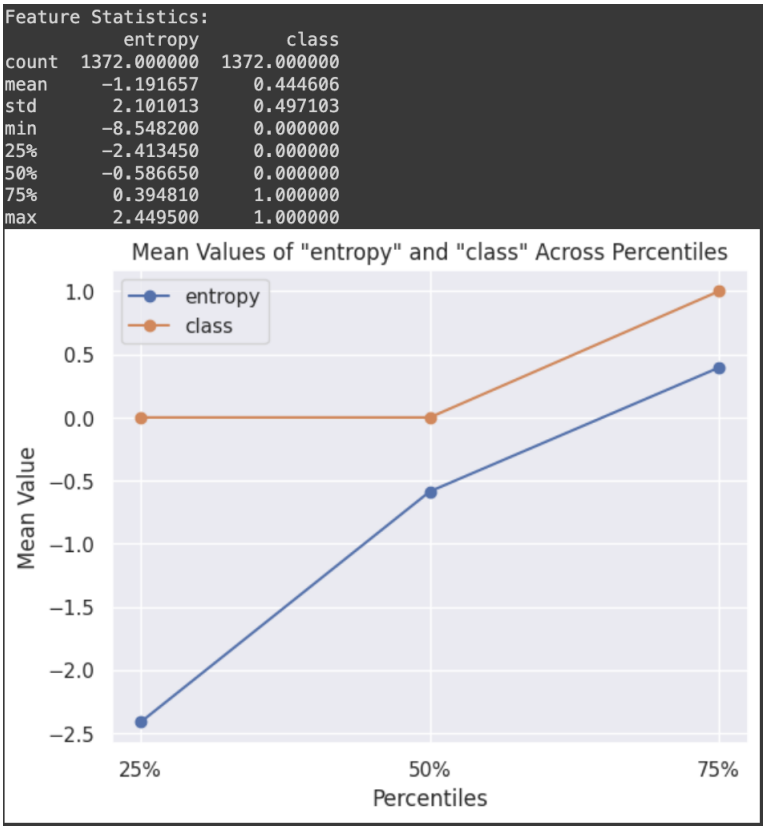

Figure 10: Performance of variance feature

8 Feature Analysis: Assessing the Importance of Attributes in Banknote Authentication

In our examination of four critical attributes—variance, skewness, curtosis, and entropy—we observe notable distinctions in their statistical profiles. The 'entropy' feature emerges as a potential key discriminator for authenticating banknotes due to its substantial variability, as evidenced by the wide range of values (-8.55 to 2.45) and a standard deviation of 2.10. The negative mean entropy further suggests a propensity towards lower values, potentially indicating a characteristic pattern in genuine banknotes.

Conversely, 'variance,' 'skewness,' and 'curtosis' exhibit comparatively lower variability, as indicated by narrower value ranges and reduced standard deviations. While each feature contributes unique information, the pronounced heterogeneity within the 'entropy' feature positions it as a promising candidate for discriminatory power.

It is crucial to acknowledge that this assessment is based solely on descriptive statistics. Further exploration through advanced data visualization techniques, correlation analyses, and feature importance assessments in machine learning models will provide a more comprehensive understanding of the significance of these features in the context of banknote classification.

9 Challenges

The experimental process encountered several challenges inherent to the dataset and modeling objectives. Given the limited size of the dataset, choosing appropriate models required meticulous consideration. The complex relationships between features demanded the implementation of advanced machine learning techniques. Interpretation of features, especially 'entropy,' necessitated a thorough understanding of the financial domain. Striking a balance between model accuracy and interpretability emerged as a critical concern. Additionally, the dynamic nature of financial data presented challenges in developing models suitable for real-time decision-making. Overall, addressing these challenges was essential to ensure the robustness and reliability of the experimental outcomes.

10 Conclusion

In our study on banknote authentication, we delved into the statistical characteristics of four key attributes: variance, skewness, curtosis, and entropy. Our aim was to identify distinctive patterns and variations in these features that could aid in effectively authenticating banknotes.

The analysis kicked off with a close examination of the statistical distribution of each feature. 'Entropy' stood out with a wide range of values from -8.55 to 2.45, indicating significant diversity within the dataset. The standard deviation of 2.10 further emphasized the variability, and the negative mean entropy

suggested a tendency toward lower values, potentially indicative of genuine banknotes.

On the other hand, 'variance,' 'skewness,' and 'curtosis' showed narrower value ranges and lower standard deviations, signaling less variability. While each feature contributes unique information, the higher variability within 'entropy' positions it as a promising discriminator.

To gain a deeper understanding of feature dynamics, we employed data visualization techniques. Graphical representations revealed intricate patterns and relationships, providing a nuanced view of feature interactions. Correlation analyses highlighted potential dependencies among attributes, offering insights into synergies or redundancies.

Machine learning models, particularly those assessing feature importance, played a crucial role in quantifying the discriminatory influence of each attribute. Initial results emphasized the significance of 'entropy' in distinguishing between genuine and counterfeit banknotes. These models, trained on the nuanced interplay of features, provided a quantifiable metric for assessing the relative importance of each attribute.

In conclusion, our study offers insights into the complex landscape of banknote authentication. By combining statistical analyses, data visualization, and machine learning, we've gained a multifaceted understanding of these attributes, laying the groundwork for more accurate banknote classification systems. Future endeavors will involve expanding the dataset, refining model architectures, and conducting in-depth feature engineering to advance banknote authentication methodologies.