Weekly Project Update Report

(Manigandan Ramadasan)

This week my main goal was to improvise the 2D CNN model by trying out different parameters and I got significant improvement in accuracy, precision, recall, and F1 score metrics and they are as follows:

Metric	**Plain Text Data (%)**	**Encrypted Data (%)**
Accuracy	96.15	96.20
Precision	95.70	95.00
Recall	96.65	97.52
F1 - Score	96.17	96.25

The model has one Convolution layer (this is limited by TenSEAL because of im2col operation) and two dense layers with square activation function after every layer and sigmoid for the last layer. The trade-off is that I had to use bigger parameters since the convolution operation in TenSEAL is achieved through im2col technique. Due to this, the multiplicative depth increases so I had to increase the value of t (=[40, 31, 31, 31, 31, 31, 31, 40]) which leads to increase in the value of n (=16384) to maintain 128-bit security and because of this the time taken to evaluate one sample increases (~0.59s).

In addition to this, I tried implementing Inverse Algorithm, Min-Max Algorithm, Comparison Algorithm based on Approximation [1]. The Inverse and Mix Max algorithm gave correct results, but the Mix Max Algorithm took more time that expected. The main challenge faced this week was with the approximation-based comparison algorithm. It didn't provide the expected output, indicating potential issues with its implementation or the approximation approach.

The foremost goal for next week is to rectify the issues with the comparison algorithm. If the approximation-based comparison algorithm is successfully corrected and provides the expected results, the next goal is to implement decision trees. Another task is to make a comparison table with different parameter for different algorithm which will be useful for concluding the best algorithm.

[1] Cheon, J. H., Kim, D., Kim, D., Lee, H. J., & Lee, K. (2019). Numerical method for comparison on homomorphically encrypted numbers. In *Lecture Notes in Computer Science* (pp. 415–445). https://doi.org/10.1007/978-3-030-34621-8_15