Abstract

High numbers of spam emails have led to an increase in email triage, causing losses amounting to USD 355 million per year. One way to reduce this loss is to classify spam email into categories including fraud or promotions made by unwanted parties. The initial development of spam email classification was based on simple methods such as word filters. Now, more complex methods have emerged such as sentence modeling using machine learning. Some of the most well-known methods for dealing with the problem of text classification are networks with Long Short Term Memory (LSTM) and Gated Recurrent Units (GRU). This study focuses on the classification of spam emails, so both the LTSM and GRU methods were used. The results of this study show that, under the scenario without dropout, the LSTM and GRU obtained the same accuracy value of 99.02%, superior to XGBoost, the base model. Meanwhile, in the dropout scenario, LSTM outperformed GRU and XGboost with each obtaining an accuracy of 98.60%, 98.58%, and 98.52%, respectively. The GRU Recall score was better than that of LSTM and XGBoost in the scenario with dropouts, each obtaining values of 98.98%, 98.92%, and 98.15% respectively. In the scenario without dropouts, LSTM was superior to GRU and XGBoost, with each obtaining values of 98.39%, 98.39%, and 98.15% respectively.

Keywords: GRU, LSTM, Spam Classification