Pclf: parallel cnn-lstm fusion model for sms spam filtering

Mohammad Reza Feizi Derakhshi1*, Elnaz Zafarani-Moattar2, Hussein Al’a Al-kabi3 and Ahmed Hashim Jawad Almarashy4

1ComInSys Lab, Department of Computer Engineering, University of Tabriz, Iran
2 Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Iran
3 Ministry of Education Iraq, General Direction Of Vocational Education, Al-Najaf, Iraq
4 Decision support and information technology department, Karbala government, Iraq

Abstract. Short Message Service (SMS) is widely used for its accessibility, simplicity, and cost-effectiveness in communication, bank notifications, and identity confirmation. The increase in spam text messages presents significant challenges, including time waste, potential financial scams, and annoyance for users and carriers. This paper proposes a novel deep learning model based on parallel structure in the feature extraction step to address this challenge, unlike the traditional models that only enhance the classifier. This parallel model fuses local and temporal features to enhance feature representation by combining convolutional neural networks (CNN) and long short-term memory networks (LSTM). The performance of this model has been evaluated on the UCI SMS Collection V.1 dataset, which comprises both spam and ham messages. The model achieves an accuracy of 99.28% on this dataset. Also, the model demonstrates good precision, recall, and F1 score. This paper aims to provide the best protection from unwanted messages for mobile phone users.

1 Introduction

The Short Message Service, shortly known as (SMS), enables easy text exchanges between mobile phones. With this development in text communication, the number of unwanted text messages has increased. These spam messages include fraudulent offers, phishing scams, and unsolicited marketing, which pose a risk to the privacy and information of the users [1]. The International Telecommunication Union reveals that more than 50% of all mobile phone users in the world receive spam messages [2]. That means we need effective SMS spam filtering solutions to protect mobile phone users from unwanted messages. While several approaches have evolved to combat unwanted SMS messages, they have misclassified problems. Most of these approaches focus on improving the classifier without improving
feature extraction from textual data. Deep learning is an essential section of artificial intelligence (AI). It's known for its impressive accuracy in various tasks like text classification [3], face recognition [4], and even detecting unusual patterns [5]. These algorithms use neural networks that work similarly to human brain neurons. For example, Convolutional Neural Networks (CNN) can effectively identify spam in emails, social media, and online reviews [6].

This paper introduces a hybrid deep learning framework for SMS spam detection using CNN and LSTM in a parallel architecture. The CNN branch extracts local features from SMS text. At the same time, the LSTM branch is used to extract the temporal features from the sentences. After this dual extraction process, early data fusion is employed to concatenate the extracted features. This fusion provides a comprehensive feature representation. Following this integration with the feature selector, and here we use the attention mechanism, the attention layer enhances the model's efficiency by selecting the most important features to optimize the classification workflow.

The local and temporal features help the SMS spam detection model understand information in two ways. Suppose the user receives a text message. Looking at specific words in this message, like "win" or "free" (these are local features), gives a hint that it might be spam. Then, by looking at how these words are arranged or the timing between similar messages (these are temporal features), it's like collecting evidence that helps the system know more about the true nature of the message. For instance, if a message "Congratulations! You win a free vacation," The combination of "win" and "free" in one message helps the model detect that it is spam. This approach increases efficiency in SMS spam detection models by using one feature type.

To evaluate the performance of the proposed model, we use the UCI Spam SMS dataset [7]. We compare our model results with traditional and deep learning methods in the literature and demonstrate their superiority in accuracy and other evaluation metrics. The main contributions of this paper are as follows:

Enhanced Feature Representation by concurrently capturing temporal and local features from SMS messages.

The proposed model outperforms other machine and deep learning algorithms in SMS spam filtering, achieving an accuracy of 99.28% on the UCI dataset.

The remainder of the paper is organized as follows: Section 2 reviews related work on SMS spam filtering. Section 3 describes the detailed architecture of our proposed model. Section 4 presents the experimental results. Finally, Section 5 concludes the paper and discusses future work.

2 Related work

This paper tries to provide a complete understanding survey of the SMS spam detection researcher by categorizing the related work into two sections: the traditional method and the deep learning method. This approach aims to provide a clear and organized overview to understand the problem statement and provide a comparison between various methodologies in the SMS spam detection challenge.

2.1 Traditional methods

There are many traditional machine learning methods for this task. These approaches include rule-based filters such as decision trees, random forests, support vector machines, and Naive Bayes classifiers [8]. However, traditional techniques often require extensive feature
engineering and may fizzle out with noisy or imbalanced data. Navaney et al. [9] proposed a supervised support vector machine algorithm for spam filtering, achieving an accuracy of 97.4% on the SMS Spam Corpus v.0.1 [7]. SVMs have limitations in dealing with noisy data and may demand complex feature engineering [10]. N. Sjarif et al. [11] introduced a method for SMS spam filtering based on the TF-IDF technique for feature extraction and the Random Forest algorithm for classification. This method achieved an accuracy of 97.5%.

Hosseinpour et al. [12] proposed an ensemble learning method based on two traditional approaches (logistic regression and random forest algorithms). The ensemble methods aren't novel, and they just combine more than one approach for one task. This ensemble learning method attained an accuracy of 98.06%. Ali et al. [13] also proposed combining traditional machine learning techniques for SMS spam detection; it uses multiple linear regression (MLR) for feature weighting and an extreme learning machine (ELM) for classification. This method achieved an accuracy of 98.7% on the UCI dataset.

2.2 Deep Learning Methods

In recent years, deep learning approaches have been widely used for text classification, and the SMS spam filtering challenge was one of them, utilizing the power of neural networks to learn features from data and handle noisy and imbalanced datasets, unlike the rule-based methods. Tian Xia et al. [14] introduced a new SMS spam detection system that includes a hidden Markov model (HMM) for capturing the sequence of words and addressing the weakness of typical frequency-based methods. This HMM approach attained an accuracy of 95.9% on the UCI dataset and 98.5% on local Chinese SMS datasets containing 2000 messages.

Kumar et al. [15] introduced a deep learning approach using convolutional neural networks for SMS spam detection. Their CNN model is used as a classifier to detect unwanted messages compared with traditional machine learning methods such as SVM, Naïve Bayes, and Random Forest, achieving an accuracy of 98.4% on the UCI SMS spam dataset.

Raj et al. [16] introduced a new model for SMS spam detection using LSTM and Word2Vec to represent simplified text as vectors in a vector space. This approach tries to make the input data more suitable before the classification step. The method attained an accuracy of 97.5%. Abayomi et al. [17] also introduced a deep learning approach using Bidirectional Long Short-Term Memory, shortly known as (BiLSTM), to identify SMS spam. Their research employed two datasets: ExAIS_SMS [18] and the UCI dataset. The approach achieved 98.6% accuracy on the UCI SMS dataset. Ghourabi et al. [19] presented a hybrid model combining CNN and LSTM sequentially to detect SMS spam in Arabic and English. Employ the CNN for feature extraction and the LSTM for classification. The proposed model is compared to traditional machine learning methods, achieving an accuracy of 98.37%. Srinivasarao et al. [20] proposed an FRNN-HHO model with a KELM classifier for text classification for the short text (SMS), the long text (Email), and sentiment analysis. The model achieved an accuracy of 98.61% on the SMS dataset and 95.8% on the email dataset.

Several studies have explored text message classification and spam detection using databases in local languages such as Persian [20] and Indonesian [21]. Some papers also focused on datasets containing images and text [22].

3 The Proposed Method
The Parallel CNN-LSTM Fusion (PCLF) model for SMS spam filtering is proposed, effectively capturing local and temporal features to classify messages as spam or non-spam. The PCLF model consists of five main steps, as shown in Figure 1.

### 3.1 Pre-processing

In the SMS spam detection framework, data pre-processing is an initial step, and the deep learning models use it to enhance analysis [23]. This pre-processing includes the removal of unnecessary punctuation and characters, reducing vocabulary size, and focusing on the meaning. We convert all text to lowercase to ensure consistency and uniform vocabulary usage, minimizing variations caused by capitalization [24]. The process also involves excluding words that occur frequently but are semantically unimportant, known as stop words, to reduce data dimensionality [23]. Furthermore, the symbols and characters, including hashtags, are excised to maintain the model's focus on pertinent information. A critical step in this process is text normalization, which is especially critical in SMS. Text messages are usually limited in length, not exceeding 100 characters. It involves converting words to their standard forms, enhancing the data's suitability for deep learning models. These pre-processing steps convert text data into digital representations, facilitating practical analysis and increasing the efficiency of SMS spam filtering technology.

![Fig. 1. PCLF Model architecture](image-url)
3.2 Parallel Feature Extraction

The proposed PCLF model employs two parallel branches for feature extraction, and this is the novel part of the suggested model, leveraging the capabilities of CNN and LSTM to enhance SMS spam detection. In the CNN branch, convolutional layers are employed to extract local features from the text of SMS messages. Each layer applies filters, convolving over the input to capture various patterns. These filters detect specific features, such as character n-grams or word-level structures [25]. This branch deals with words to identify commonly used spam indicators like the words "winner" or "free."

Recently, spammers have tried to use a different writing style or change the word sequences in the message to avoid spam detection systems. For that, the LSTM branch is employed with the CNN branch to deal with the sentences. Concurrently, the LSTM is designed to capture long-term features. This branch processes the text sequentially, analyzing the relationships between words and phrases over time [26]. The memory cells and gating mechanisms of LSTM allow it to effectively understand the meaning behind SMS messages. It excels at identifying more intricate spam patterns, such as the catchy language that spammers frequently use. For example, in the sentence "Get a free vacation now!" the LSTM can recognize the potentially suspicious combination of "free" and "vacation" and often classify it as a spam message.

3.3 Feature Fusion

Before showing the data fusion role in this step, let's define it and know its types. Data fusion refers to the procedure of merging multiple sources of data to collect information that is clearer, more accurate, and more valuable than what can be obtained from any one data source. There are two types of it: Early fusion can generate a truly multimedia feature representation since all the features are merged from the beginning. Late fusion, also known as decision fusion, generates decisions after fusing the results of many classifiers. In our model, we employ early fusion to concatenate the extracted features. [27]. Early data fusion combines the temporal features from the LSTM branch and the local features from the CNN branch, integrating different features extracted by different tools from the text of SMS messages, giving the model more efficiency in detecting spam messages. By combining the features of CNN and LSTM through early data fusion, the model leverages the strengths of both approaches simultaneously.

3.4 Feature Selection

The attention mechanism was employed to focus on the most important features and reduce dimensions [28]. This layer assigns different importance scores to different features, with the model focusing on the most useful aspects of the data. After feature fusion via the CNN and LSTM branches, the attention layer checks these features, identifying and prioritizing those most relevant for accurate spam detection. This feature selection step helps to focus on the meaningful and important extracted features to improve accuracy in the classification process. Also, the attention layer reduces the risk of misclassification in the process.
### 3.5 Classification

In the classification stage, we employ the fully connected layer as a classifier because of its efficiency in separating the fused features that are passed through it [29], which learns the relationships between the features to identify the message according to the label to spam and non-spam. The PCLF algorithm is explained in detail in Algorithm 1.

Algorithm 1: PCLF Model for SMS Spam Detection

1. Pre-processing (Data):
   - Standardize text: lowercase conversion, remove punctuation and symbols, and stop words. Normalize text.

2. Parallel Feature Extraction:
   - CNN branch:
     - Apply convolutional layers to extract local features from SMS text.
     - For each layer, use filters to capture N-gram patterns.
     - Identify spam indicators (e.g., "winner," "free")
   - LSTM branch:
     - Use LSTM layers for sequential processing of text.
     - Analyse relationships between words over time.
     - Capture long-term features and intricate spam patterns (e.g., "Get a free vacation now!").

3. Feature Fusion:
   - Employ early fusion to concatenate local and temporal features from CNN and LSTM branches for comprehensive representation.

4. Feature Selection:
   - Utilize the Attention Mechanism to prioritize features based on relevance for effective spam detection and dimension reduction.

5. Classification:
   - Use a Fully Connected Layer as a Classifier:
   - Learn relationships between features.
   - Classify messages into spam and non-spam categories.

### 4 Evaluation

#### 4.1 Dataset Description:

The UCI SMS Spam Collection v.1 dataset is sourced from the UCI Machine Learning Repository. It comprises 5,574 English text messages, 4,827 instances (86.6%) classified as legitimate, and 747 instances (13.4%) as spam. This imbalanced dataset type reflects real-world scenarios. The distribution of the dataset is visually represented in Figure 2.
4.2 Data splitting

We divided the UCI SMS dataset into training and testing sets to evaluate our model's performance. The dataset was randomly split, with 80% of the data allocated for training and the remaining 20% for testing, as shown in Figure 3. The 80-20 split for training and testing ensures enough data for model training, good generalization, overfitting prevention, and alignment with standard field practices.
4.3 Data training

The proposed SMS spam filtering model employs the training data to calibrate the model's parameters and reduce the loss function [30]. Utilizing batch processing, the model progressively adjusts its parameters to improve its precision in categorizing SMS messages. In this study, we iteratively trained a deep learning model to achieve optimal performance. This involved repeatedly presenting the model with training data, allowing it to learn and refine its parameters. To assess its effectiveness, we evaluated the model on a separate set of unseen data, mimicking real-world application scenarios. This optimization process aimed to identify the perfect configuration that yielded the highest performance. Importantly, the training and optimization procedures were implemented using Python 3.7, a widely-used programming language, while leveraging the computational power and memory capacity of a robust computer equipped with an Intel Core i7 CPU and 16 GB of RAM.

The LSTM branch utilizes a layer with 128 units, enabling it to capture temporal features and understand the sequential nature of the input data. On the other hand, the CNN branch employs a one-dimensional convolutional layer using 128 filters and a kernel size of 3, extracting local features from the input. This design efficiently captures local patterns in the data. The kernel size of 3 is optimal for immediate context analysis, while the 128 filters enable a broad and detailed feature extraction, balancing model complexity and computational efficiency. Through early data fusion, the extracted features from both branches are combined, capitalizing on the respective strengths of CNN and LSTM to capture local patterns and contextual dependencies, consequently enhancing the model's predictive capabilities. The output layer of the model comprises two units, representing spam and ham classifications, and employs a softmax activation function for effective classification [31].

4.4 Performance metric

When evaluating the performance of deep learning models, let's first understand four fundamental terms:

<table>
<thead>
<tr>
<th>Table 1 Confusion matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual</td>
</tr>
<tr>
<td>Spam</td>
</tr>
<tr>
<td>Spam</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Ham</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Accuracy**: Reflects the model's overall correct classifications of spam and non-spam. It's the proportion of accurate predictions (TP and TN) and general predictions (TP, FP, TN, FN), calculated as:

\[
\text{Accuracy} = \frac{(TP + TN)}{(TP + FP + TN + FN)}
\]  

(1)

**Precision**: Indicates the accuracy of spam predictions, which is essential for minimizing false positives. Calculated as:

\[
\text{Precision} = \frac{TP}{(TP + FP)}
\]  

(2)
Recall: Measures the model's success in identifying spam, aiming to reduce missed spam. It's the ratio of TP to all actual spam cases (TP + FN), calculated as:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

F1-score: Harmonizes precision and recall, which is useful for balancing the two. It's the harmonic mean of precision and recall, calculated as:

$$\text{F1 score} = \frac{2 \times (\text{Recall} \times \text{Precision})}{(\text{Recall} + \text{Precision})} \tag{4}$$

These metrics comprehensively evaluate the model's ability to detect SMS spam, considering its overall accuracy and effectiveness in differentiating spam and non-spam messages.

5 Result and Analysis

This study comprehensively evaluated our proposed PCLF model for SMS spam detection, comparing it against several contemporary methodologies, including the modified Transformer, FRNN-HHO, CNN-LSTM BUNOW, BERT, and CNN-LSTM. This assessment, detailed in Table 2, focused on key performance metrics: accuracy, precision, recall, and F-measure. The PCLF model demonstrated superior performance, achieving an accuracy rate of 99.28%, precision of 0.998, recall of 0.997, and an F-measure of 0.998.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>97.4%</td>
<td>0.92</td>
<td>0.94</td>
<td>0.95</td>
</tr>
<tr>
<td>RF</td>
<td>97.5%</td>
<td>0.98</td>
<td>0.97</td>
<td>0.98</td>
</tr>
<tr>
<td>HHM</td>
<td>95.9%</td>
<td>0.97</td>
<td>0.89</td>
<td>0.91</td>
</tr>
<tr>
<td>FRNN-HHO</td>
<td>98.6%</td>
<td>0.99</td>
<td>0.98</td>
<td>0.98</td>
</tr>
<tr>
<td>CNN</td>
<td>98.4%</td>
<td>0.95</td>
<td>0.93</td>
<td>0.93</td>
</tr>
<tr>
<td>LSTM</td>
<td>97.5%</td>
<td>0.95</td>
<td>0.96</td>
<td>0.96</td>
</tr>
<tr>
<td>Sequential CNN-LSTM</td>
<td>98.37 %</td>
<td>0.95</td>
<td>0.87</td>
<td>0.91</td>
</tr>
<tr>
<td>Parallel CNN-LSTM</td>
<td>99.28%</td>
<td>0.99</td>
<td>0.99</td>
<td>0.98</td>
</tr>
</tbody>
</table>

Figure 4 provides a visual representation of the comparative accuracy assessment of these models using the UCI SMS Spam Collection v.1 dataset; the PCLF model outperformed all other methods with a 99.28% accuracy rate.
Fig. 4. Performance comparison

The confusion matrix [33], as shown in Figure 5, shows the PCLF model's accuracy in spam and non-spam message classification. Also, the confusion matrix shows the suggested model has a minimal misclassification rate.

Fig. 5. Confusion matrix
The high level of accuracy and precision demonstrates the effectiveness of the PCLF model. Evaluation using a standard random data split of 80% to 20% ensures a realistic assessment of the model's capabilities in typical usage scenarios. The proposed model has limitations in multi-language datasets.

6 Conclusion And Future Work

This paper introduces a novel approach, the Parallel CNN-LSTM Fusion Model (PCLF), designed for SMS spam filtering. The model aims to improve feature representation and enhance spam detection accuracy. They combine the power of LSTM and CNN simultaneously to capture more than one feature type and then use early data fusion. Combine the extracted features into a new form that enhances greater accuracy in text classification. Experimental evaluation on a UCI SMS dataset has shown that the proposed model outperforms state-of-the-art approaches, achieving a good accuracy of 99.28%. These results show the impact of the PCLF model on effectively filtering SMS spam and protecting mobile phone users from unwanted messages. Future research will explore extending the PCLF model to multilingual SMS datasets and adapting it for longer text formats such as emails, aiming to broaden its applicability and enhance its spam detection capabilities across various languages and communication platforms.

References


