Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.034841
Article

Tech Science Press

Improved Fruitfly Optimization with Stacked Residual Deep Learning Based Email Classification

Hala J. Alshahrani[1], Khaled Tarmissi[2], Ayman Yafoz[3], Abdullah Mohamed[4], Abdelwahed Motwakel[5,*], Ishfaq Yaseen[5], Amgad Atta Abdelmageed[5] and Mohammad Mahzari[6]

[1]Department of Applied Linguistics, College of Languages, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[2]Department of Computer Sciences, College of Computing and Information System, Umm Al-Qura University, Makkah, 24211, Saudi Arabia
[3]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 22230, Saudi Arabia
[4]Research Centre, Future University in Egypt, New Cairo, 11845, Egypt
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, 16242, Saudi Arabia
[6]Department of English, College of Science & Humanities, Prince Sattam bin Abdulaziz University, AlKharj, 16242, Saudi Arabia
*Corresponding Author: Abdelwahed Motwakel. Email: a.ismaeil@psau.edu.sa
Received: 29 July 2022; Accepted: 26 October 2022

Abstract: Applied linguistics means a wide range of actions which include addressing a few language-based problems or solving some language-based concerns. Emails stay in the leading positions for business as well as personal use. This popularity grabs the interest of individuals with malevolent intentions—phishing and spam email assaults. Email filtering mechanisms were developed incessantly to follow unwanted, malicious content advancement to protect the end-users. But prevailing solutions were focused on phishing email filtering and spam and whereas email labelling and analysis were not fully advanced. Thus, this study provides a solution related to email message body text automatic classification into phishing and email spam. This paper presents an Improved Fruitfly Optimization with Stacked Residual Recurrent Neural Network (IFFO-SRRNN) based on Applied Linguistics for Email Classification. The presented IFFO-SRRNN technique examines the intrinsic features of email for the identification of spam emails. At the preliminary level, the IFFO-SRRNN model follows the email pre-processing stage to make it compatible with further computation. Next, the SRRNN method can be useful in recognizing and classifying spam emails. As hyperparameters of the SRRNN model need to be effectually tuned, the IFFO algorithm can be utilized as a hyperparameter optimizer. To investigate the effectual email classification results of the IFFO-SRDL technique, a series of simulations were taken placed on public datasets, and the comparison outcomes highlight the enhancements of the IFFO-SRDL method over other recent approaches with an accuracy of 98.86%.

Keywords: Email classification; applied linguistics; improved fruitfly optimization; deep learning; recurrent neural network

1 Introduction

Recently, bulk emails related to commercial purposes have been known as spam, becoming a great problem over the internet [1]. The individual who sends the spam messages is called the spammer. This individual gathers email addresses from several websites, viruses, and chatrooms [2,3]. Spam thwarts the user from making good and complete use of time, network bandwidth, and storage capability. The massive volume of spam mail flows via the networks has negative effects on the storage space of email servers [4], computer processing unit (CPU), power user time, and communication bandwidth [5]. There was an increase in the threat of spam email year by year, accounting for nearly 77% of the total global email traffic. Users seem to be annoyed when they receive spam emails they did not request [6]. It also leads to ineffable monetary loss to several users those experiences internet scams and other fraudulent acts of spammers by whom the spam emails are sent, and they send spam emails to reputable companies to persuade individuals to disclose personal data such as credit card numbers, passwords, and Bank Verification Number (BVN). Natural Language Processing (NLP) is a subfield of artificial intelligence (AI) that permits machines to operate natural human languages. NLP was used in several domains [7]. In this study, the steps of classifying an email, whether spam or not, utilise NLP methods. The ease of interacting with the arrival of email caused the issue of unsolicited bulk emails, particularly phishing attacks through emails [8]. Several anti-phishing methods were advanced to solve the issue of phishing assaults. This study focused on segregating significant emails from spam [9]. One key factor for classification is the ways in which the messages will be represented. To be specific, one has to decide which feature to use and how it has to be used when classifying them [10]. Several authors have used AI in intelligent systems, most of which employed Deep learning (DL) in cybersecurity applications.

Douzi et al. [11] introduce a hybrid technique for spam filtering relevant to the NN method of Paragraph Vector-Distributed Memory (PV-DM). The author utilizes PV-DM to constitute a compact representing an email context and its appropriate features. This method indicates a more comprehensive filter to classify Emails. Shuaib et al. [12] modelled the usage of a metaheuristic optimizing technique, the whale optimization algorithm (WOA), for choosing prominent features in the email corpus and rotation forest technique to categorize emails as spam from non-spam. The complete datasets have been employed, and the assessment of the rotation forest method is executed previously and after selecting features with WOA. Anitha et al. [13] devised an improvised spam exposure model related to Extreme Gradient Boosting (XGBoost) approach. It can be learned for higher accuracy in detecting spam. And it is anticipated trivial considerations of spam e-mail detection complexities.

Saleh [14] proposes the integration of the Chaotic particle swarm optimization (PSO) method with Artificial Bees Colony (ABC) to minimize the dimensionality of features in a bid to enhance spam emails classifier accuracy. The structures for every particle in this study have been indicated in a binary format, that they are transmitted into binary utilizing a sigmoid function. Selecting the features depends on a fitness function that relies on the gained accuracy utilizing a support vector machine (SVM). In [15], the author tried identifying spam mail and filtering it at the time of their communication. The Author devised a Collaborative filtering method hybridized with text classification (semantics related). The related feature was retrieved from text content. Additionally,

another content-related filtering technique can be presented that segregates the same spam mail with better and higher accuracy. In addition to the semantic texts, Content-related filtering will filter the specialized symbols like @, HTML tags, /, and many more.

Rajendran et al. [16] present one method which employs a hybrid technique for effective spam detection. A collaborative spam filtering structure utilizing extraction of the fingerprints of the layout and complete email layout can be suggested for matching and catching the spam sprouting nature. The collaborative structure employs references from other end-users for creating spam databases. The incoming mail was checked in contrast to the spam database for spam categorization utilizing a close duplicate similarity matching method. To minimize false negative and positive ratios in classifying spam, the author computes cumulative weights from fingerprints as well as email layouts. Fingerprint signs of new spam, classified, were increasingly upgraded to the spam databases for up-to-date detecting of spam. Gaurav et al. [17] designed a new spam mail detecting approach related to the document labelling concept that makes a classification the newer one into spam or ham. In addition, methods such as random forest (RF), Naive Bayes (NB), and decision tree (DT) were utilized in the process of classification.

This paper presents an Improved Fruitfly Optimization with Stacked Residual Recurrent Neural Network (IFFO-SRRNN) based Applied Linguistics for Email Classification. The presented IFFO-SRRNN technique examines email's intrinsic features for identifying spam emails. At the preliminary level, the IFFO-SRRNN model follows email pre-processing stage to make it compatible with further computation. Next, the SRRNN method can recognise and classify spam emails. As hyperparameters of the SRRNN model need to be effectually tuned, the IFFO algorithm can be utilized as a hyperparameter optimizer. A series of simulations were carried out on a public dataset to investigate the effectual email classification results of the IFFO-SRDL technique.

2 The Proposed Model

In this paper, a novel IFFO-SRRNN methodology has been devised to recognise and classify emails. The presented IFFO-SRRNN algorithm examines the intrinsic features of email for the identification of spam emails. Fig. 1 depicts the block diagram of IFFO-SRRNN approach.

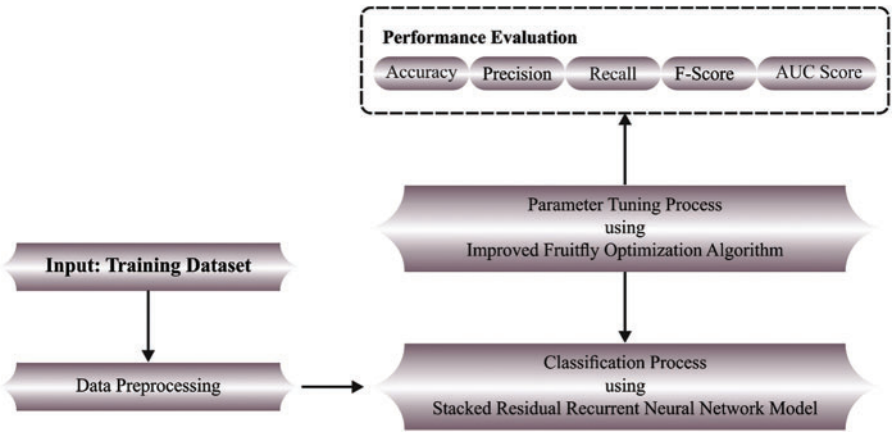

Figure 1: Block diagram of IFFO-SRRNN approach

2.1 Email Pre-processing

At the preliminary level, the IFFO-SRRNN model follows email pre-processing to make it compatible with further computation. An email contains certain properties for classifying legitimate emails (ham), spam, phishing, or other groups [18]. An email is provided in various file formats; thus, property extraction must be ready. But for email classification, few added processing is employed for obtaining some particular features. For instance, a divide phishing email-based features into 2 major groups: website features and email features. The features belonging to Email were based on emails the metadata and data and classified into attachment data, header, and body. At the same time, website features were based on the data that was collected from the email body and connected to it. The features of the website depended upon the link. Whereas many solutions depend on the data that is straightforwardly collected through email (the link uniform resource locator (URL) provided as internet protocol (IP), without a domain name or address; the number of various fields in the links; and so on.), few solutions even examine the website itself (script code; the website content; etc.) or utilize certain additional tools for validating the URL.

2.2 Email Classification Using SRRNN Technique

In this study, the SRRNN technique can be utilized to recognise and classify spam emails. Layer stacking is a conventional method for adding representation power to neural networks [19]. RNN stacking was effectively employed in various research. But the stacking layer of neural network (NN) suffers from degradation problems. This is because of the complexity of training multiple stacked layers and fitting those layers to underlying mapping, resulting in representation degradation.

The solution presented to these problems is the residual connection attempts to generate shortcuts among non-consecutive layers. However, the residual connection (add the input vector to the hidden depiction) add numerous limitations on the dimensionality of the input and hidden units that may need vector clipping, and it could result in data loss.

The novel residual connection is developed for recognizing images, and the residual data is added to the output of upper layer $(F(x) + x)$. In this study, we require the upper layer of NN to have direct access to the novel input; therefore, the novel input is attached to the output of lower layer rather than being added. Using these data, there exists no dimensionality constraint, and we argued that the presented residual connection is utilized for mixing feature learners of distinct complications. For instance, once it is armed with the presented residual connection, the upper NN layer acts as a shallower one-layer feature learner. The two upper layers act are a deep two-layer feature learner. Eq. (1) illustrates the exact formula of the presented residual connection within the Stacked RNN. Fig. 2 demonstrates the infrastructure of Bi-RNN. It represents the Bi-RNN function as ρ and the concat function as ψ.

$$
\begin{aligned}
&h_0^0, \ldots, h_n^0 = \rho\left(x_0, \ldots, x_n\right) \\
&\hat{h}_0^0, \ldots, \hat{h}_n^0 = \psi\left(\left[x_0, h_0^0\right]\right), \ldots, \psi\left(\left[h_n^0, x_n\right]\right) \\
&h_0^1, \ldots, h_n^1 = \rho\left(\hat{h}_0^0, \ldots, \hat{h}_n^0\right) \\
&h_0^M, \ldots, h_n^M = \rho\left(\hat{h}_0^{M-1}, \ldots, \hat{h}_n^{M-1}\right)
\end{aligned} \tag{1}
$$

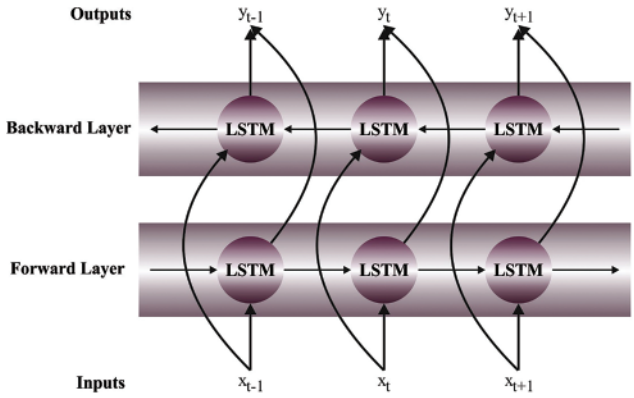

Figure 2: Framework of Bi-RNN

2.3 Hyperparameter Tuning

At last, the IFFO algorithm is used as a hyperparameter optimizer. In order to define global optimization parameters, FFOA is essentially used on the basis of food-finding behaviors of fruit flies [20]. For feature extraction and selection, we employ IFFO, which efficiently helps to select considerable features and enhances the efficiency of feature selection. Among several species, fruit flies (FFs) are superior in sensing and perception, particularly in osphresis. Along with vision, osphresis organ smells each variety of odours in the environment, and even food source is far from 40 km distance. Then, to get close to the food position, it exploits sensitive vision to find its flocking location of company and food and flies in that direction. The random walking in FFOA is replaced with Levy Flight (LF) behaviours to diminish the computation effort. Therefore, this FFOA can be called an IFFO. In this study, the extracted feature is inputted to the IFFO and the steps are expounded and enumerated in the following.

Step 1: Allocate the population of FF group as M_{in}, N_{in}.

Step 2: Implement random searching for direction and distance via osphresis of FFs. Estimate the direction and distance of the fruit flies as follows:

$$M_i = M + R_d, \tag{2}$$

$$N_i = N + R_d, \tag{3}$$

where

M_i—Position of *i-th* FF,

N_i—Direction of *i-th* FF,

R_d-Random number.

Rather than exploiting the random searching technique, the LF behaviour is applied to get the improved feature value. The LF is a random walking while the steps were usually determined based on the length. It follows a likelihood distribution where the direction of steps must be isotropic and random.

$$Levy\ (\lambda) = t\,(-\lambda)\,,\ 1 < \lambda < 3, \tag{4}$$

In Eq. (4), t denotes task completion time, and λ denotes random walk.

Step 3: The food position is unknown; hence, we determined the distance D_i, which is evaluated as follows. Estimate the concentration of smell judgment value by considering the reciprocal of distance as follows:

$$D_i = \sqrt{M_i^2 + N_i^2}. \tag{5}$$

Calculate the smell concentration using Eq. (6)

$$SC_i = \frac{1}{D_i}. \tag{6}$$

Step 4: Guess the Objective Function (OF) with respect to SC_i, and the maximal smell is assumed as fitness. It is estimated in the following:

$$OB_i = \delta_{\max} + \delta_{\min} + \frac{F}{n}\sum\nolimits_{k=1}^{n} |Ou_k - Ou_k^w|, \tag{7}$$

where

OB_j-Objective Function or Smell concentration of the *i-th* fruit flies,

n-Overall amount of training instance.

OB_i refers to contingent on the judgment value of smell concentration. The OF value focus on the maximal fitness values, whereas O_k^w indicates the class value of the ground dataset, Ou_k specifies the predictable output for feature extraction, and F represents the regularization factor:

$$\delta = eigen\left(W \times W^T\right), \tag{8}$$

$$\delta_{\max} = \max\ (\delta),\ \delta_{\min} = \min\ (\delta). \tag{9}$$

Step 5: Estimate the optimal FFs with the maximal smell concentration that can be shown in the following:

$$F_{best} = \text{Max}\ (SC_i). \tag{10}$$

The maximum values of the smell can be preserved when the FF uses the vision that might move in the direction of the position which is corresponding to the maximum smell:

$$\text{Max}\ (SC) = bestsmell. \tag{11}$$

The position and direction of the FF that provides the maximum value of the smell are shown below.

$$M = M_i\ —best, \tag{12}$$

$$N = N_i—best. \tag{13}$$

Step 6: the process is repeated for steps 2 through 5, and if the smell is higher than the smell judgment value of previous iteration, later keep the previous iteration values; otherwise, go with the search technique.

Algorithm 1: Pseudocode of FFO

```
Begin
    Initialize the place of the FF group as M_in, N_in
    for every extracted feature, do
        Random walk utilizing Eq. (4)
    end for
    for every feature, do
        Calculate the objective function by utilizing Eq. (7)
    end for
    Calculate the optimal FF using Eq. (10)
    Calculate direction and position utilizing Eqs. (12) and (13)
    Repeat the above steps
    If smell value > smell judgment value, then
        Retain the smell value
    else
        Repeat the smell values
End
```

3 Performance Validation

The email classification results of the IFFO-SRRNN method are investigated on an email dataset. The dataset holds 692 spam and 182 phishing emails, as shown in Table 1.

Table 1: Dataset details

Class	No. of emails
Spam	692
Phishing	182
Total number of emails	**874**

Fig. 3 reports the confusion matrices formed by the IFFO-SRRNN method. On 80% of training (TR) data, the IFFO-SRRNN algorithm has recognized 533 samples under the spam class and 143 samples under the Phishing class. Also, on 20% of testing (TS) data, the IFFO-SRRNN method has recognized 140 samples under spam class and 33 samples under the Phishing class. Otherwise, on 70% of TR data, the IFFO-SRRNN approach has recognized 467 samples under spam class and 122 samples under the Phishing class. Finally, on 30% of TS data, the IFFO-SRRNN algorithm has recognized 212 samples under spam class and 42 samples under the Phishing class.

A brief email classification outcome of the IFFO-SRRNN model on 80% of TR data and 20% of TS data is exhibited in Table 2. Fig. 4 highlights the classifier results of the IFFO-SRRNN model on 80% of TR data. The results inferred the IFFO-SRRNN method has attained enhanced classification results. For instance, in spam class, the IFFO-SRRNN model has attained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and Mathew Correlation Coefficient (MCC) of 96.71%, 98.89%, 96.91%, 97.89%, 96.44%, and 90.54% respectively. Along with that, in phishing class, the IFFO-SRRNN approach has gained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 96.71%, 89.38%, 95.97%, 92.56%, 96.44%, and 90.54% correspondingly.

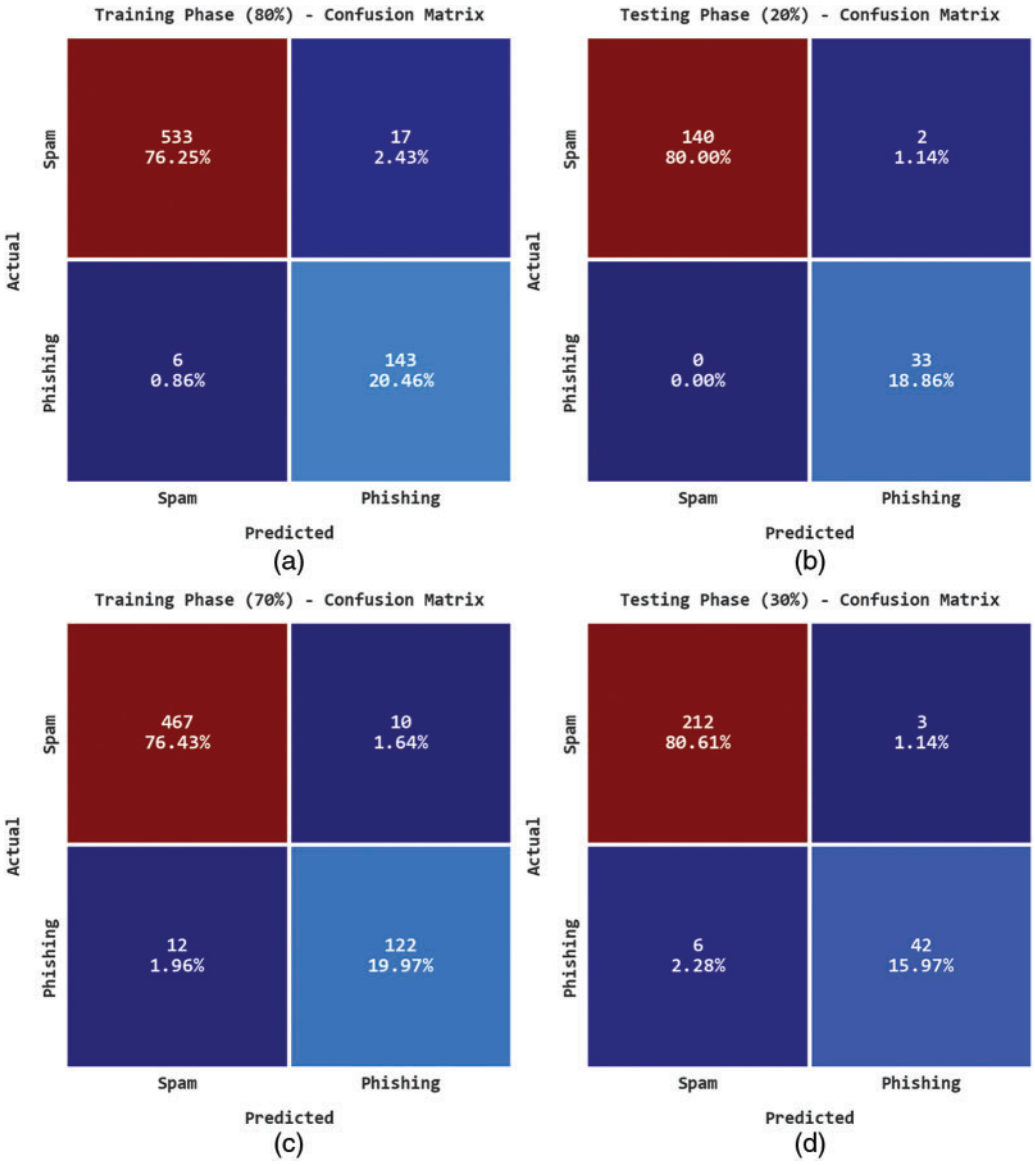

Figure 3: Confusion matrices of IFFO-SRRNN approach (a) 80% of TR data, (b) 20% of TS data, (c) 70% of TR data, and (d) 30% of TS data

Fig. 5 portrays the classifier results of the IFFO-SRRNN approach on 20% of TS data. The results inferred that the IFFO-SRRNN method has attained enhanced classification results. For instance, in spam class, the IFFO-SRRNN algorithm has obtained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 98.86%, 100%, 98.59%, 99.29%, 99.30%, and 96.41% correspondingly. In addition, in phishing class, the IFFO-SRRNN, methodology has acquired $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 98.86%, 94.29%, 100%, 97.06%, 99.30%, and 96.41% correspondingly.

Table 2: Result analysis of IFFO-SRRNN approach under 80:20 of TR/TS data

Labels	Accuracy	Precision	Recall	F-Score	AUC score	MCC
Training phase (80%)						
Spam	96.71	98.89	96.91	97.89	96.44	90.54
Phishing	96.71	89.38	95.97	92.56	96.44	90.54
Average	**96.71**	**94.13**	**96.44**	**95.22**	**96.44**	**90.54**
Testing phase (20%)						
Spam	98.86	100.00	98.59	99.29	99.30	96.41
Phishing	98.86	94.29	100.00	97.06	99.30	96.41
Average	**98.86**	**97.14**	**99.30**	**98.17**	**99.30**	**96.41**

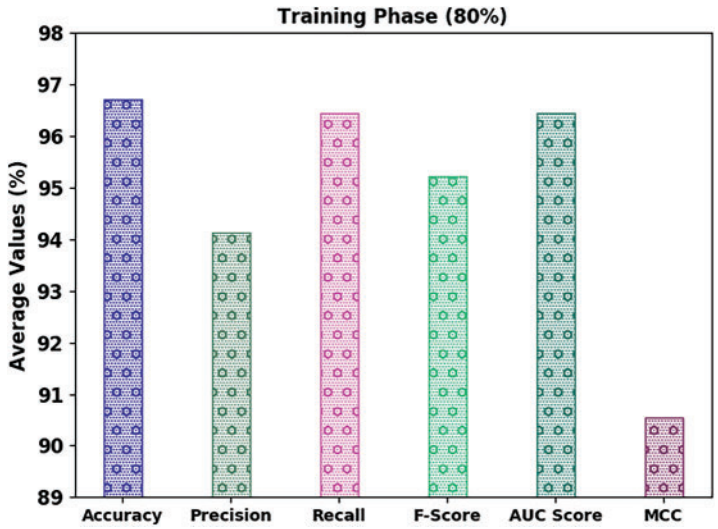

Figure 4: Average analysis of IFFO-SRRNN approach under 80% of TR data

A brief email classification outcome of the IFFO-SRRNN method on 70% of TR data and 30% of TS data is shown in Table 3. Fig. 6 emphasizes the classifier results of the IFFO-SRRNN approach on the 70% of TR data. The results implicit in the IFFO-SRRNN method have gained enhanced classification results. For example, in spam class, the IFFO-SRRNN method has acquired attained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 96.40%, 97.49%, 97.90%, 97.70%, 94.47%, and 89.43% correspondingly. Additionally, in phishing class, the IFFO-SRRNN approach has reached attained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 96.40%, 92.42%, 91.04%, 91.73%, 94.47%, and 89.43% correspondingly.

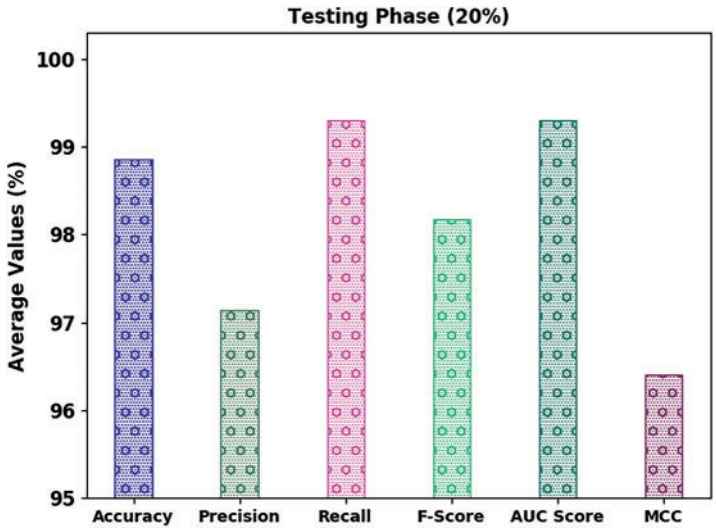

Figure 5: Average analysis of IFFO-SRRNN approach under 20% of TS data

Table 3: Result analysis of IFFO-SRRNN approach under 70:30 of TR/TS data

Labels	Accuracy	Precision	Recall	F-Score	AUC score	MCC
Training phase (70%)						
Spam	96.40	97.49	97.90	97.70	94.47	89.43
Phishing	96.40	92.42	91.04	91.73	94.47	89.43
Average	**96.40**	**94.96**	**94.47**	**94.71**	**94.47**	**89.43**
Testing phase (30%)						
Spam	96.58	97.25	98.60	97.92	93.05	88.31
Phishing	96.58	93.33	87.50	90.32	93.05	88.31
Average	**96.58**	**95.29**	**93.05**	**94.12**	**93.05**	**88.31**

Fig. 7 displays the classifier results of the IFFO-SRRNN approach on 30% of TS data. The outcomes inferred the IFFO-SRRNN method had gained enhanced classification results. For example, in spam class, the IFFO-SRRNN model has attained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 96.58%, 92.75%, 98.60%, 97.92%, 93.05%, and 88.31% correspondingly. In addition, in phishing class, the IFFO-SRRNN model has reached attained $accu_y$, $prec_n$, F_{score}, AUC_{score}, and MCC of 96.58%, 93.33%, 87.50%, 90.32%, 93.05%, and 88.31% correspondingly.

The training accuracy (TRA) and validation accuracy (VLA) acquired by the IFFO-SRRNN methodology on the test dataset is shown in Fig. 8. The experimental result implicit the IFFO-SRRNN approach has achieved maximal values of TRA and VLA. Seemingly the VLA is greater than TRA.

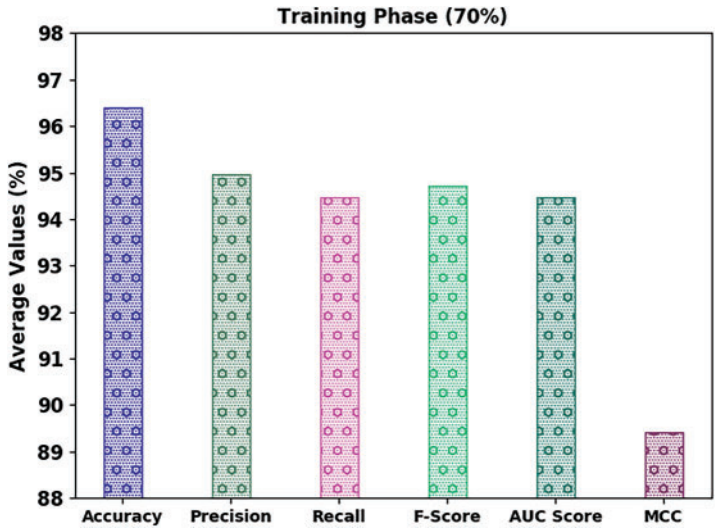

Figure 6: Average analysis of IFFO-SRRNN approach under 70% of TR data

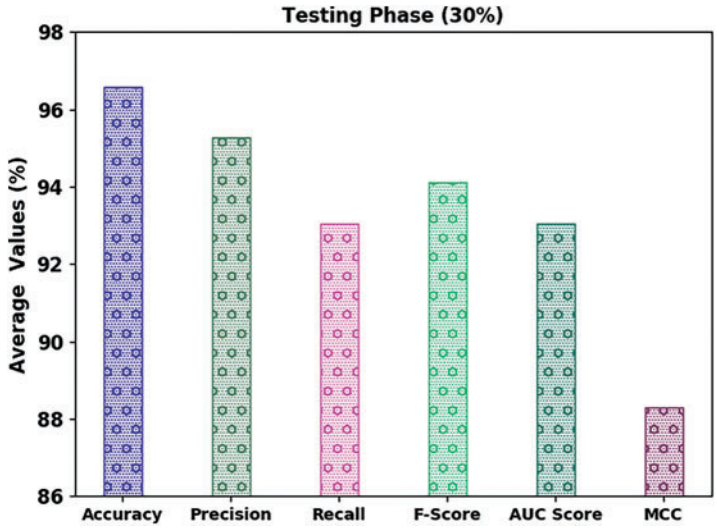

Figure 7: Average analysis of IFFO-SRRNN approach under 30% of TS data

The training loss (TRL) and validation loss (VLL) attained by the IFFO-SRRNN method on the test dataset are presented in Fig. 9. The experimental result denoted the IFFO-SRRNN method exhibited minimal values of TRL and VLL. Particularly, the VLL is lesser than TRL.

Figure 8: TRA and VLA analysis of the IFFO-SRRNN approach

Figure 9: TRL and VLL analysis of the IFFO-SRRNN approach

A clear precision-recall analysis of the IFFO-SRRNN technique on the test dataset is portrayed in Fig. 10. The figure denoted the IFFO-SRRNN methodology has resulted in enhanced values of precision-recall values in all classes.

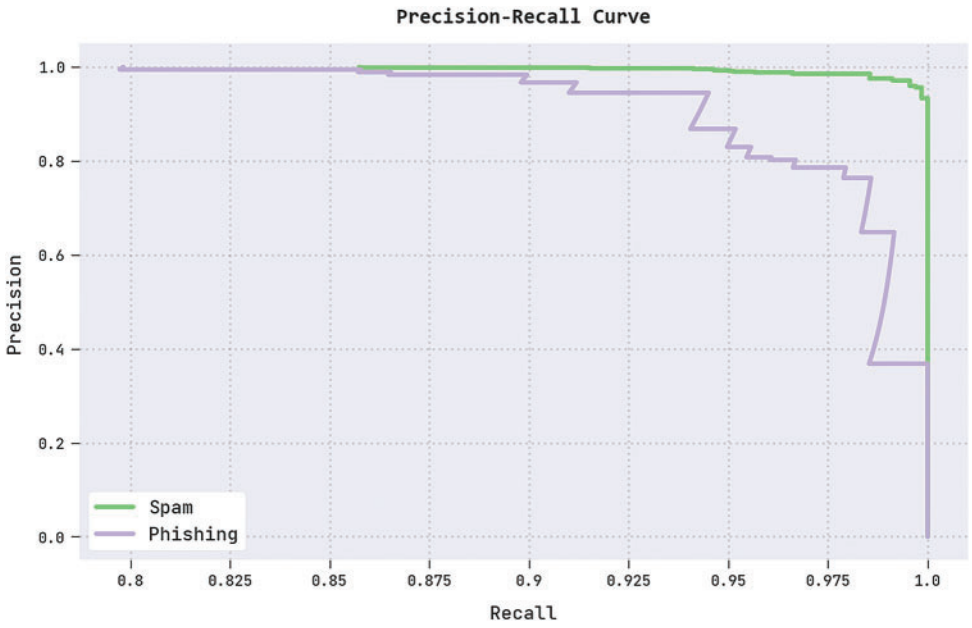

Figure 10: Precision-recall analysis of the IFFO-SRRNN approach

A brief ROC analysis of the IFFO-SRRNN method on the test dataset is exhibited in Fig. 11. The results indicated the IFFO-SRRNN method had shown its capability in classifying distinct classes on the test dataset.

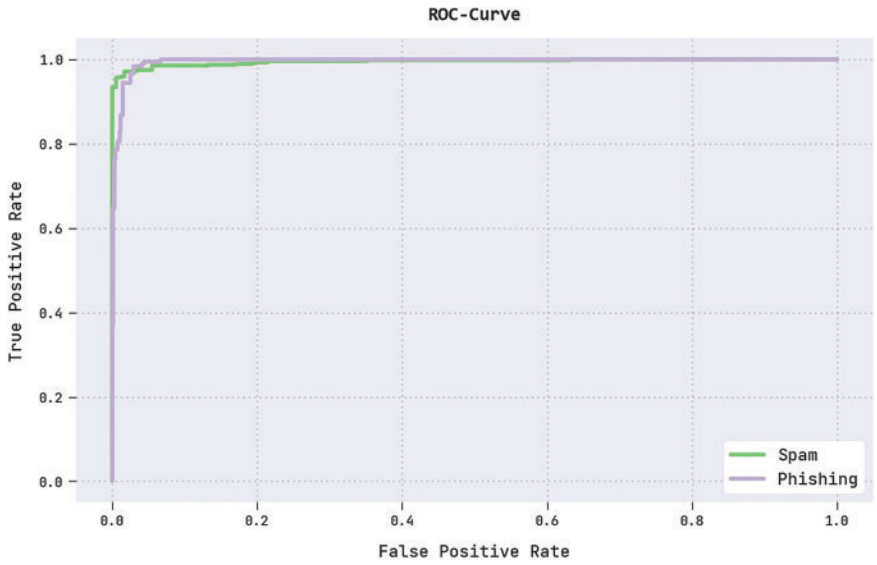

Figure 11: ROC analysis of the IFFO-SRRNN approach

The comparative email classification outcomes of the IFFO-SRRNN model with recent models are made in Table 4. The obtained values indicated that the IFFO-SRRNN model had shown enhanced outcomes under all measures [18].

Table 4: Comparative analysis of the IFFO-SRRNN approach with existing methodologies

Methods	Accuracy	Precision	Recall	F score	AUC
Naïve bayes	59.67	93.39	20.93	35.26	67.84
Linear model	83.25	80.06	88.75	83.58	89.50
Fast large margin	83.00	78.97	90.49	84.43	93.03
GB trees	57.60	93.59	13.72	23.95	98.21
SVM model	83.46	78.60	95.31	86.12	92.15
IFFO-SRRNN	98.86	97.14	99.30	98.17	99.30

Fig. 12 reports a detailed $accu_y$ assessment of the IFFO-SRRNN model with recent approaches. The results demonstrated that the gradient boosting trees (GBTrees) and NB models had shown poor performance with minimal $accu_y$ of 57.60% and 59.67%. Followed by the linear model, Fast large margin and SVM models have obtained moderately closer $accu_y$ of 83.25%, 83%, and 83.46%, respectively. But the IFFO-SRRNN model has shown enhanced performance with a maximum $accu_y$ of 98.86%.

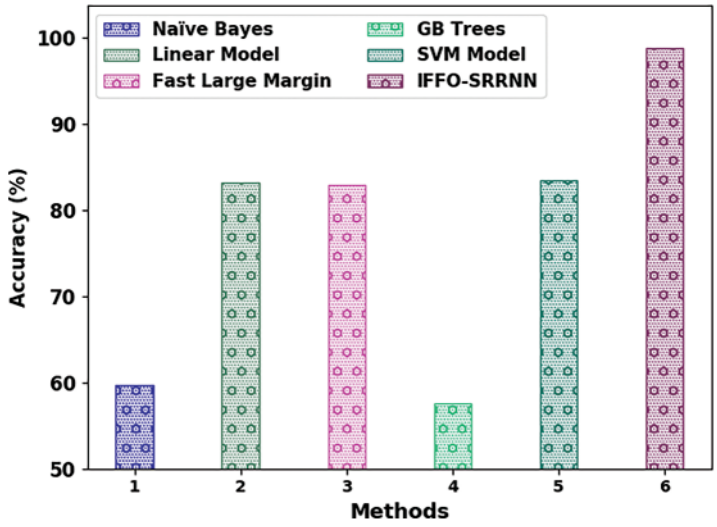

Figure 12: *Accu*$_y$ analysis of IFFO-SRRNN approach with existing methodologies

Fig. 13 demonstrates a brief $pren_c$ assessment of the IFFO-SRRNN technique with recent approaches. The results denoted that the GBTrees, and NB algorithms have exhibited poor performance with minimal $pren_c$ of 93.59% and 93.39%. then, the linear model, Fast large margin, and SVM techniques have gained moderately closer $pren_c$ of 80.06%, 78.97%, and 78.60%, correspondingly. But the IFFO-SRRNN approach has exhibited enhanced performance with maximum $pren_c$ of 97.14%.

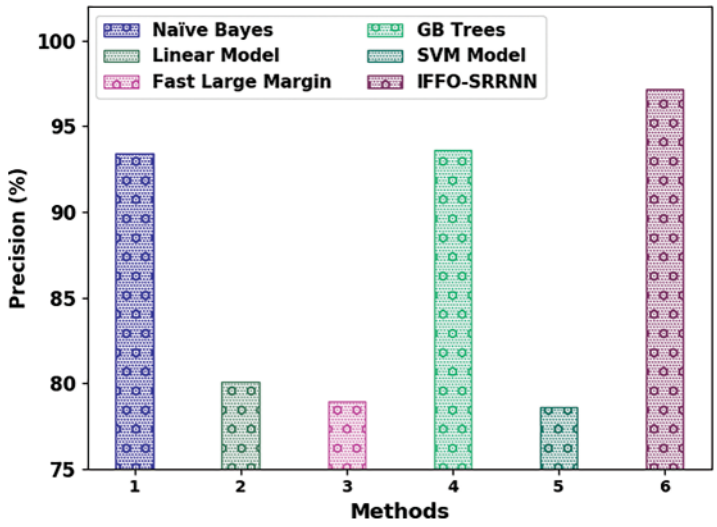

Figure 13: *Pren*$_c$ analysis of IFFO-SRRNN approach with existing methodologies

Fig. 14 illustrates a compressive *reca*$_l$ assessment of the IFFO-SRRNN approach with recent approaches. The results represented the GBTrees, and techniques have established poor performance with minimal *reca*$_l$ of 13.72% and 20.93%. Next, the linear model, Fast large margin, and SVM approaches have reached moderately closer *reca*$_l$ of 88.75%, 90.49%, and 95.31%, correspondingly. But the IFFO-SRRNN method has displayed enhanced performance with maximum *reca*$_l$ of 99.30%.

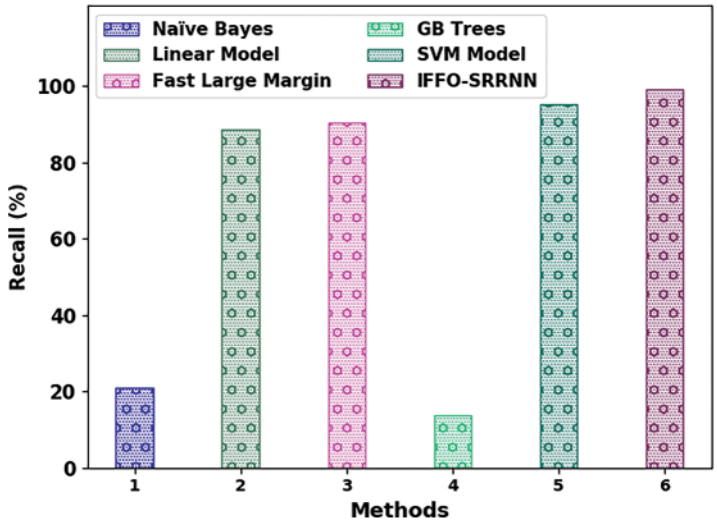

Figure 14: *Reca*$_l$ analysis of IFFO-SRRNN approach with existing methodologies

4 Conclusion

In this article, a new IFFO-SRRNN method has been projected for the recognition and classification of emails. The presented IFFO-SRRNN algorithm examines the intrinsic features of email for the identification of spam emails. At the preliminary level, the IFFO-SRRNN model follows

email pre-processing stage to make it compatible for further computation. Next, the SRRNN methid can be employed for the recognition and classification of spam emails. As hyperparameters of the SRRNN model need to be effectually tuned, the IFFO algorithm is used as hyperparameter optimizer. To investigate the effectual email classification results of the IFFO-SRDL technique, a series of simulations were performed on public dataset and the comparison outcomes highlight the enhancements of the IFFO-SRDL methodology over other recent approaches with accuracy of 98.86%. In the future, the presented IFFO-SRRNN approach was tested on large scale real time email datasets.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R281), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4331004DSR31).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. G. Dada, J. S. Bassi, H. Chiroma, A. O. Adetunmbi and O. E. Ajibuwa, "Machine learning for email spam filtering: Review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, pp. e01802, 2019.

[2] H. Yang, Q. Liu, S. Zhou and Y. Luo, "A spam filtering method based on multi-modal fusion," *Applied Sciences*, vol. 9, no. 6, pp. 1152, 2019.

[3] I. Tamhankar and M. R. Bhatiya, "An analysis on email classification on hindi language using Bayesian classifier," *Journal of Artificial Intelligence, Machine Learning and Neural Network (JAIMLNN)*, vol. 2, no. 4, pp. 29–35, 2022.

[4] T. Gangavarapu, C. D. Jaidhar and B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: Review and approaches," *Artificial Intelligence Review*, vol. 53, no. 7, pp. 5019–5081, 2020.

[5] F. Z. Ruskanda, "Study on the effect of preprocessing methods for spam email detection," *Indonesia Journal on Computing (Indo-JC)*, vol. 4, no. 1, pp. 109–118, 2019.

[6] G. H. AL-Rawashdeh and R. B. Mamat, "Comparison of four email classification algorithms using WEKA," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 2, pp. 42–54, 2019.

[7] M. Jazzar, R. F. Yousef and D. Eleyan, "Evaluation of machine learning techniques for email spam classification," *International Journal of Education and Management Engineering*, vol. 11, no. 4, pp. 35–42, 2021.

[8] O. E. Taylor and P. S. Ezekiel, "A model to detect spam email using support vector classifier and random forest classifier," *International Journal of Computer Science and Mathematical Theory*, vol. 6, no. 1, pp. 1–11, 2020.

[9] W. Li, L. Ke, W. Meng and J. Han, "An empirical study of supervised email classification in internet of things: Practical performance and key influencing factors," *International Journal of Intelligent Systems*, vol. 37, no. 1, pp. 287–304, 2022.

[10] M. A. Mohammed, D. A. Ibrahim and A. O. Salman, "Adaptive intelligent learning approach based on visual anti-spam email model for multi-natural language," *Journal of Intelligent Systems*, vol. 30, no. 1, pp. 774–792, 2021.

[11] S. Douzi, F. A. AlShahwan, M. Lemoudden and B. Ouahidi, "Hybrid email spam detection model using artificial intelligence," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 316–322, 2020.

[12] M. Shuaib, S. I. M. Abdulhamid, O. S. Adebayo, O. Osho, I. Idris *et al.,* "Whale optimization algorithm-based email spam feature selection method using rotation forest algorithm for classification," *SN Applied Sciences*, vol. 1, no. 5, pp. 1–17, 2019.
[13] P. U. Anitha, C. G. Rao and D. S. Babu, "Email spam filtering using machine learning based XGBoost classifier method," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 11, pp. 2182–2190, 2021.
[14] H. M. Saleh, "An efficient feature selection algorithm for the spam email classification," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 9, no. 3, pp. 520–531, 2021.
[15] S. P. Shyry and Y. B. Jinila, "Detection and prevention of spam mail with semantics-based text classification of collaborative and content filtering," *Journal of Physics: Conference Series*, vol. 1770, no. 1, pp. 012031, 2021.
[16] P. Rajendran, A. Tamilarasi and R. Mynavathi, "A collaborative abstraction based email spam filtering with fingerprints," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1913–1923, 2022.
[17] D. Gaurav, S. M. Tiwari, A. Goyal, N. Gandhi and A. Abraham, "Machine intelligence-based algorithms for spam filtering on document labeling," *Soft Computing*, vol. 24, no. 13, pp. 9625–9638, 2020.
[18] J. Rastenis, S. Ramanauskaitė, I. Suzdalev, K. Tunaitytė, J. Janulevičius *et al.,* "Multi-language spam/phishing classification by email body text: Toward automated security incident investigation," *Electronics*, vol. 10, no. 6, pp. 668, 2021.
[19] W. Cao, A. Song and J. Hu, "Stacked residual recurrent neural network with word weight for text classification," *IAENG International Journal of Computer Science*, vol. 44, no. 3, pp. 277–284, 2017.
[20] T. Bezdan, C. Stoean, A. A. Naamany, N. Bacanin, T. A. Rashid *et al.,* "Hybrid fruit-fly optimization algorithm with k-means for text document clustering," *Mathematics*, vol. 9, no. 16, pp. 1929, 2021.