The Journal of Computational Science and Engineering.
ISSN: 2583-9055

Enhancing Spam Detection: Leveraging Deep Convolutional Neural Networks and Transfer Learning for Image-Based Spam Identification

Bonu Satish Kumar[1], Kopanati Shankar[2], Sailaja Vishnubhatla[3], A Sumathi[4]

[1] Department of Computer Science, SVA GDC, Srikalahasthi, India.
[2]Department of Computer Science and Engineering, NSRIT, Visakhapatnam AP India.
[3] Department of Computer Science, GDC, Ravulapalem, India.
[4] Department of Computer Science, GDCW Degree College SKHT, Srikalahasti, INDIA,

Received on: 17-12-2023 Accepted on: 28-02-2024

Keyword:
Image Spam Detection,
Cyber Security,
Deep Convolutional networks,
Transfer Learning

ABSTRACT

In modern cyber threats, attackers increasingly utilize image-based spam techniques as conventional methods primarily target textual content and hyperlinks. Addressing this challenge, our research employs Deep Convolutional Neural Networks (DCNNs) in conjunction with pre-trained architectures for image classification, a field that has seen rapid advancement in recent years. However, the computational demands of training robust image classification models pose significant challenges. Leveraging transfer learning, we mitigate these constraints by fine-tuning pre-trained models on specific image datasets. Our proposed approach demonstrates superior performance to existing state-of-the-art models in identifying image-based spam content, achieving both heightened accuracy and efficiency

Corresponding Author: Email: Kopanati@gmail.com

1. Introduction

The rise of the Internet in recent times owes much to its cost-effective nature, prompting a surge in online social activity. Users flock to virtual communities for various purposes, propelled by a quest for popularity, often oblivious to the criminal underbelly of social media. This eagerness to join social platforms has unwittingly exposed many to nefarious activities orchestrated by cyber attackers. Unlike the past, where spam primarily manifested in textual form, modern spammers have evolved, leveraging images to captivate users' attention and propagate their agendas.In their pursuit, attackers employ a variety of tactics, including product/service promotions, fake giveaways, phishing scams, and malware distribution, all disseminated through deceptive images containing user-targeted content. Traditional machine learning techniques, effective against text-based spam, have been outpaced by these evolving tactics [1]. Consequently, efforts have shifted towards detecting image spam, initially relying on optical character recognition and subsequently adopting deep learning methodologies [2].

Deep learning models offer significant promise due to their ability to automatically extract features and recognize patterns. They typically consist of convolutional and pooling layers, facilitating efficient feature selection and extraction. However, the complexity of deep learning models necessitates time-consuming feature extraction processes. Transfer learning emerges as a valuable tool in this context, leveraging pre-trained models to expedite development and reduce computational costs [3-7]. This paper focuses on classifying images into ham (legitimate) and spam categories using various deep learning models, employing transfer learning to optimize efficiency. Performance evaluations across different pre-trained models such as VGG16, VGG19, ResNet50, and Inception V3 are conducted using multiple datasets, including the Image Spam Hunter dataset, Dredze dataset, and an Improved dataset. The study presents novel CNN-based techniques aimed at achieving superior accuracy in image spam detection, surpassing current state-of-the-art methodologies [8].

The primary structure of this work is delineated as follows: Development of "DCNN" models for image spam detection utilizing diverse datasets. Implementation of "Transfer learning" techniques employing pre-trained models to enhance effectiveness. Provision of dataset descriptions to facilitate understanding. Elaboration on methodology and implementation details for comprehensive insight. Presentation of results and conclusions, emphasizing the significance of the research. Historically, extensive research has focused on combating text, links, and email spam, yet the realm of image spam detection remains relatively underexplored. Figure 1 showcases examples of spam images [9-15].

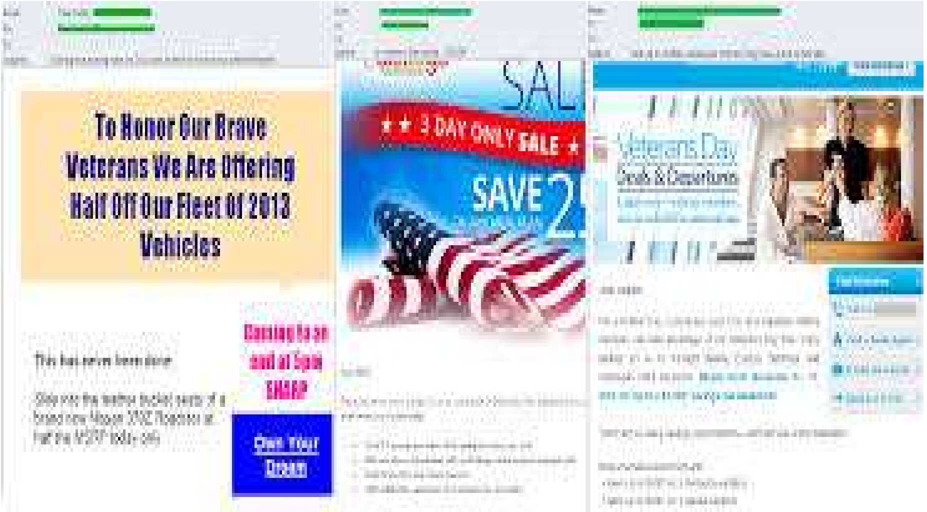

To Honor Our Brave Veterans We Are Offering Half Off Our Fleet Of 2013 Vehicles
This has never been done
Slide into the leather bucket seats of a brand new Nissan 370Z Roadster at half the MSRP today only
Closing in on end of 5pm SHARP
Own Your Dream
SALE
3 DAY ONLY SALE
SAVE 2
Veterans Day Deals & Departures

Fig 1. Sample Spam image

2.Literature Survey

Various researchers have contributed significantly to the field of image spam detection by exploring a range of techniques and datasets. Here are summaries of some of their findings:F. Gargiulo and C. Sansone (2008) [16] utilized two sets of features to identify spam images from the UNINA and DREDZE datasets. Their approach involved employing visual features and OCR-based features fed into a decision tree. They achieved impressive accuracies, with visual features scoring 94.31% and OCR features 94.79%. Their proposed approach achieved an accuracy of 97% and an F1 Score of 0.97.Shen et al. (2015) [17] developed a novel system called RoBoTs based on an efficient learning sample selection scheme and ensemble method using random forest and linear discriminative analysis. They achieved an accuracy of 96.8% for the Dredze dataset.Makkar et al. (2021) [18] constructed an optimized framework named PROTECTOR, assigning a rank score to each image and proposing an image filtering scheme to analyze image features and detect spam images. They utilized the Image Spam Hunter dataset and achieved an accuracy of 96%.

Sharmin et al. (2020) [19] employed CNN to detect image spam techniques, utilizing the ISH dataset, Challenge dataset 1, and Challenge dataset 2. They experimented with raw images, Canny images, and novel combinations of the two, with CNN outperforming SVM and achieving an accuracy of 99.02%.

Guk Nam et al. [20] blended textual and visual data to enhance image spam filtering efficiency. They utilized optical character recognition, latent Dirichlet allocation, and word2Vec methodologies for feature extraction from images, achieving an accuracy of 0.9814.

Kumaresan et al. [21] employed an S-Cuckoo spam classification framework with a hybrid kernel-based support vector machine (HKSVM). They extracted features from emails, including both textual and image-based components, achieving an impressive accuracy level of 97.235%.These studies collectively showcase diverse methodologies for detecting image spam, ranging from feature-based approaches to the application of deep learning techniques, all contributing to the enhancement of accuracy and efficiency in image spam detection systems.

3. Methodology

3.1. Pre-processing

In our study, we encountered challenges with corrupt and duplicate files across the three datasets utilized. To address this issue, we implemented a hashing technique. This involved generating unique hash values for each image and identifying instances where multiple images shared the same hash value. Subsequently, redundant images were excluded from the dataset. Following this duplication process, we aimed to establish a consistent and standardized dataset. To achieve this, all remaining unique images underwent a two-step process: normalization and resizing[22-25]. This procedure ensured a uniform appearance for the images while achieving the desired dimensions. The proposed framework is illustrated in Figure 2

3.2 Datasets and Data Augmentation

In our work, we utilized the following datasets:

A. Image Spam Hunter Dataset (ISH):

- This publicly available dataset contains both ham and spam images and can be accessed from the North-western University website [26].
- It comprises a total of 810 ham and 929 spam images. However, due to duplicates, the dataset was refined to include 879 unique ham images and 810 unique spam images.

B. Improved Images Dataset:

- This dataset consists of a total of 1029 spam images, out of which 975 are unique.
- It was employed to enhance the performance of image spam models by incorporating more advanced spam images [27].

C. Dredze Image Spam Dataset:

- This dataset, referenced as [28], comprises three distinct sets of images, each serving a specific purpose.
- The first set, labeled as Personal Ham (PHam), contains 2,021 images, out of which 1,517 are unique.
- The second set, designated as Personal Spam (PSpam), includes 3,298 images, with 1,274 being unique.
- The third set, Spam Archive (SpamArch), is extensive, containing 16,028 files of various formats (JPEG, PNG, GIF, etc.).
- Among these diverse files, there are 3,039 unique images that contribute to the dataset.

These datasets were instrumental in our research for training and evaluating image spam detection models, providing a comprehensive range of spam and ham images for analysis.

3.3 Convolutional Neural Network

In this research paper, we utilized Convolutional Neural Networks (CNNs) for image classification tasks, implementing the model architecture using the Keras API with the TensorFlow backend. The network architecture consists of multiple layers contributing to the overall classification process.First Layer (Convolutional Layer):Initiated with 8 filters of varying sizes.Applied activation using the Rectified Linear Unit (ReLU) function, introducing non-linearity to the network.For optimization, we employed the Adam optimizer with a learning rate set at 0.001. The binary cross-entropy loss function was used to measure loss and guide the training process.The architectural setup reflects our approach to leveraging CNNs for image classification within the specified framework. We built, trained, and validated a sequential 4-layer CNN model on the two-class Image Spam Hunter dataset. Training time for one epoch averaged 15 minutes on an Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz with 8GB RAM. Consequently, only five epochs were performed. Figure 3 illustrates the CNN with 4 layers, displaying accuracy and loss metrics.

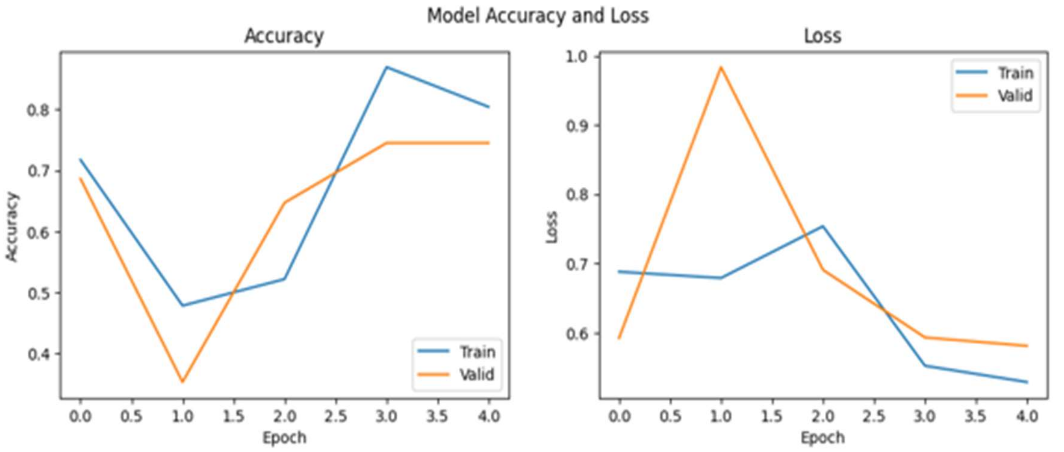


Fig2 CNN with 4 layers

3.4 Transfer learning

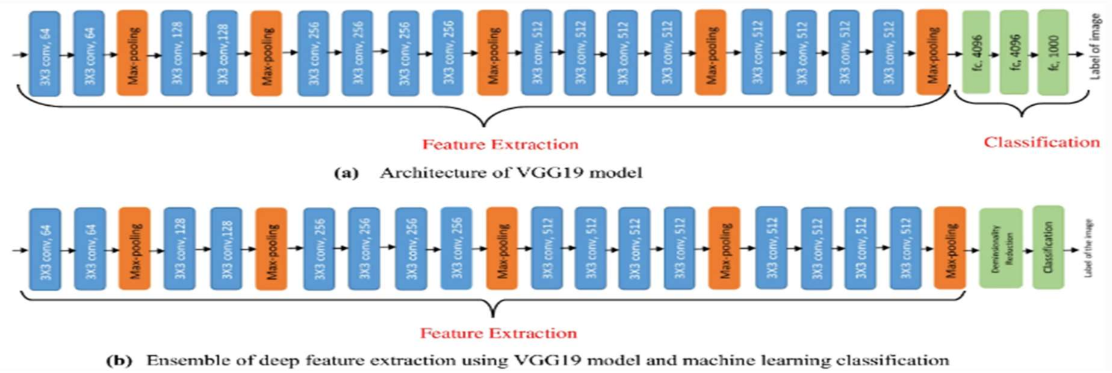
Transfer learning is a machine learning technique that involves reusing a pretrained model instead of training a new one from scratch. This approach enables the model to leverage knowledge gained from solving one problem and apply it to another, resulting in faster training times as the model has already learned to recognize relevant features in the data. In our research, we employed pretrained models and weight architectures to address our problem, specifically utilizing pretrained weights from VGG16, VGG19, ResNet50, and InceptionV3.

VGG16:

The VGG16 architecture is characterized by its deep structure comprising 16 layers, including convolutional layers followed by fully connected layers. Key features of the VGG16 architecture include:Architecture Depth: VGG16 consists of 13 convolutional layers (including five max-pooling layers) followed by three fully connected layers.Convolutional Layers: These layers use small (3x3) filters with a stride of 1 and fixed padding size of 1, enabling the network to learn increasingly complex and abstract features.Max-Pooling Layers: Employing max-pooling layers with a pool size of (2,2) downsamples the spatial dimensions of feature maps, reducing computation and controlling overfitting.Fully Connected Layers: The final layers of the network are responsible for making predictions based on learned features from previous layers.Activation Function: ReLU (Rectified Linear Unit) activation function is applied after each convolutional and fully connected layer, introducing non-linearity to the network.Output Layer: Typically consists of SoftMax activation for multiclass classification tasks, yielding class probabilities [29].

VGG19:

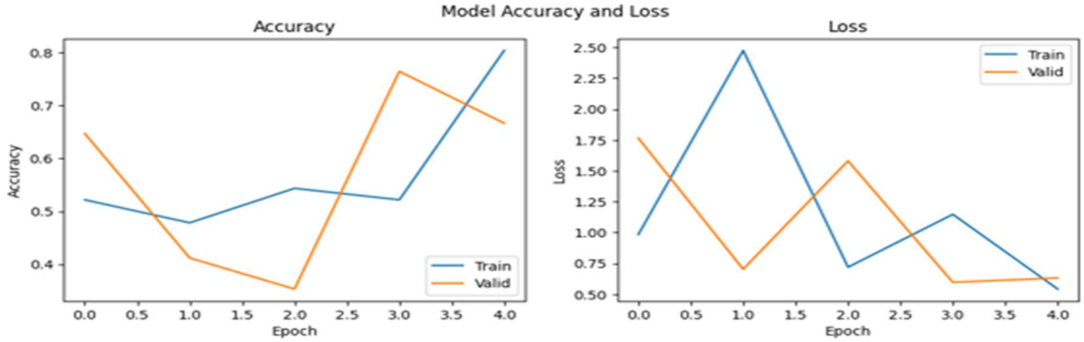
VGG19 is a deep neural network architecture comprising 19 layers, including 16 convolutional layers and 3 fully connected layers. It was trained on the extensive ImageNet dataset for image classification tasks. Key aspects of VGG19 architecture include:Convolutional Layers: Utilize 3x3 kernels with a stride of 1 pixel and spatial padding to maintain original spatial dimensions of input images.Max Pooling: Employ a 2x2 max pooling approach with a stride of 2 pixels for downsampling.Activation Function: ReLU activation function enhances both model performance and computational efficiency.Visual representations of VGG architectures are provided in Figure 5, while Figure 6 displays metrics related to accuracy and loss.



(a) Architecture of VGG19 model

(b) Ensemble of deep feature extraction using VGG19 model and machine learning classification

Fig 3. VGG19 architecture



•

Fig 4. VGG19 Accuracy and loss

3.4.3 Resnet50

The ResNet50 model refers to a specific convolutional neural network architecture with 50 layers that is generally used for numerous computer vision tasks, including “image classification, object detection”, and more. It's a part of the ResNet (Residual Network) family of models, which introduced the concept of residual blocks to address the vanishing ‘gradient problem’ in deep neural networks. Figure 7 visually displayed metrics related to accuracy and loss.

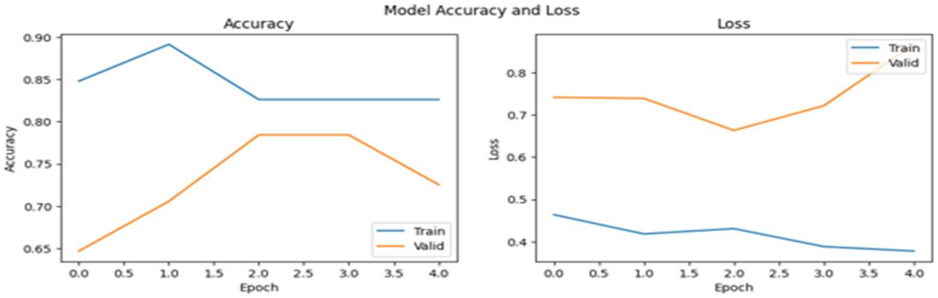


Fig 5. Resnet50 Accuracy and loss

3.4.4 InceptionV3

Transfer learning with InceptionV3 involves taking the pre-trained model and re-training its last layers on a new dataset. The initial layers of the model have already learned general features like edges, lines, and shapes, which are likely to be useful for a wide range of image classification tasks. By re-training the last layers on a specific dataset, the model can learn to recognize more specific features related to that dataset, and achieve high accuracy on the new task with less data and training time. Figure 8 visually displayed metrics related to accuracy and loss.

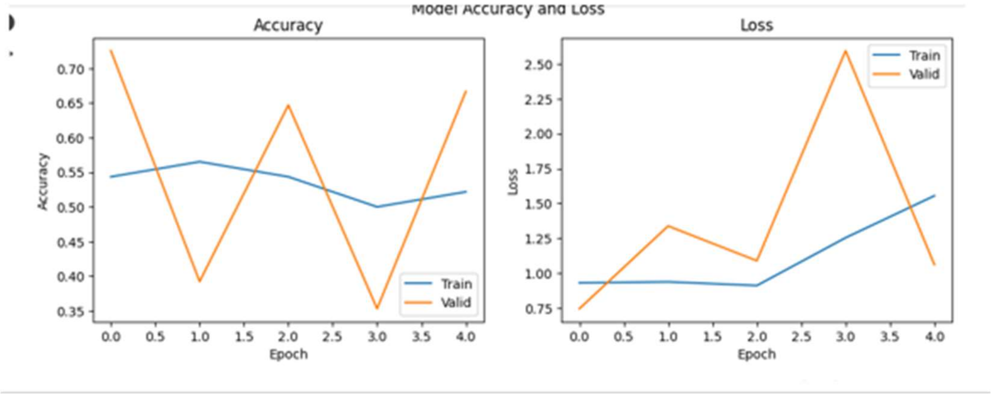


Fig 6. Inceptionv3 Accuracy and loss

3.5 Data Augmentation

In our research paper, we employed the "Data Augmentation" technique to augment the size and diversity of the training dataset. This technique involves transforming or modifying existing data samples, resulting in a new dataset with slightly altered versions of the original data. The objective of data augmentation is to create additional training samples that capture the same underlying patterns and concepts as the original dataset but with slight variations. This process helps make the model more robust and improves its ability to generalize unseen data during training.Various augmentation techniques were applied to our dataset, including flipping horizontally or vertically, rotation, translation, scaling, cropping, shearing, adding noise, and adjusting brightness, contrast, or saturation. These augmentation strategies were implemented to increase the diversity of the dataset and enhance the model's ability to learn different variations of the input data.

The impact of these augmentation strategies on the performance of diverse transfer learning models was documented and analyzed. Figures 9, 10, 11, 12, and 13 visually depict how data augmentation influences accuracy and loss metrics within the context of various transfer learning models. These figures provide insights into the effectiveness of data augmentation in improving the performance of the models across different tasks and datasets.

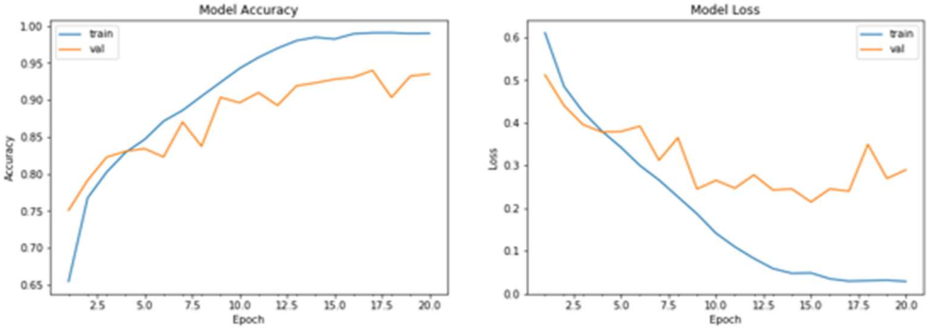


Fig 7. CNN After Data Augmentation

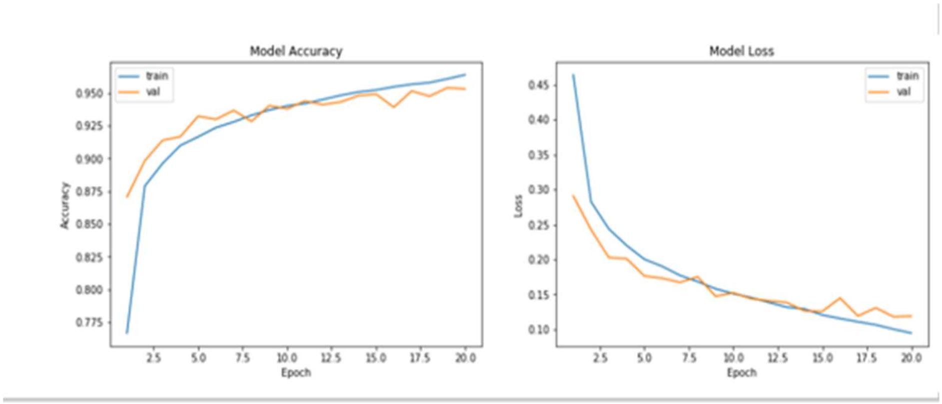


Fig 8. VGG16 After Data Augmentation

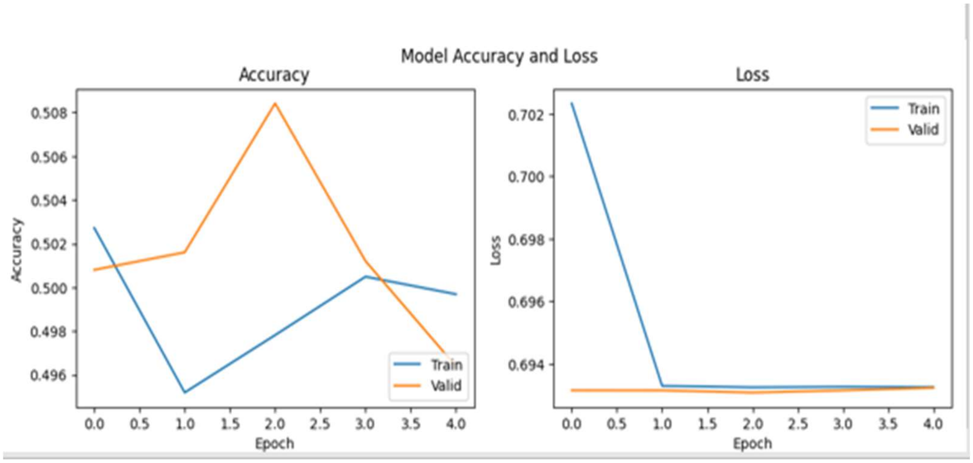


Fig 9. VGG19 After Data Augmentation

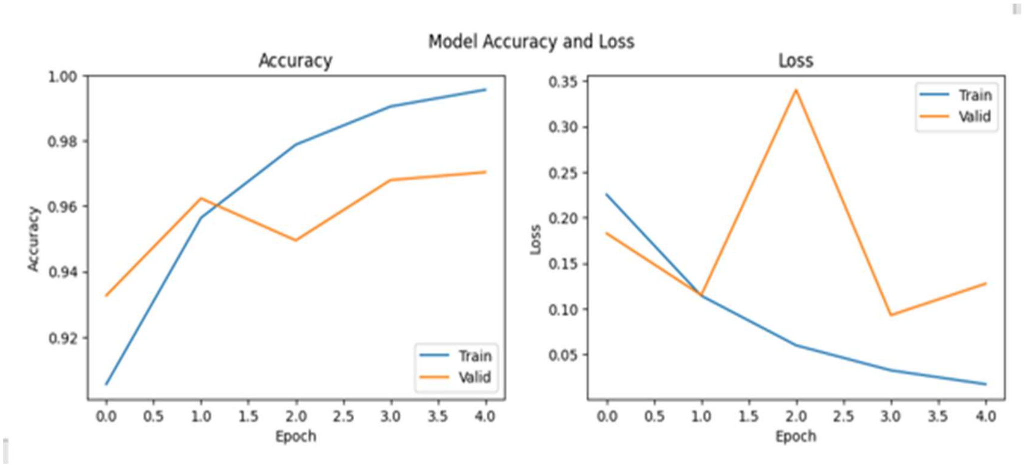


Fig 10. Resnet50 After Data Augmentation

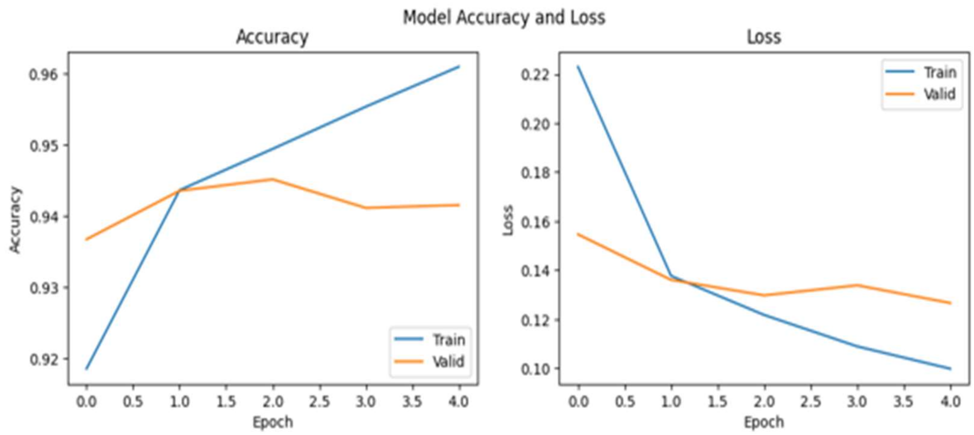


Fig 11. IneptionV3 After Data Augmentation

4. Experimental Result and Discussion

In this paper, we employed several training models, including VGG16, VGG19, Inception, and ResNet50, utilizing Google Colab for implementation. Our study utilized the Keras and Scikit-learn Python libraries for model development. To optimize the learning process, we utilized the binary cross-entropy loss function along with the Adam optimizer. Dropout regularization was incorporated to prevent overfitting.The dataset used in our study was partitioned into a 70:30 ratio, with 70% for training and 30% reserved for testing. We trained and evaluated our proposed models, namely CNN1 and CNN2, using images resized to a resolution of 128x128 pixels. This resolution was determined through experimentation across various input dimensions. Our proposed models were trained and evaluated on the Image Spam Hunter dataset, the Dreeze dataset, and an enhanced dataset over 10 epochs.The outcomes of these models are systematically presented in Table 1, showcasing the performance of the models with and without data augmentation on the Image Spam Hunter Dataset. Our proposed models consistently outperformed existing ones. Additionally, the performance of pre-trained architectures, as listed in Figure 14 and Figure 15, is visually represented. Notably, with images resize to 128x128 pixels, ResNet50 demonstrated superior performance compared to other models. Our proposed ResNet50 model, augmented with data augmentation techniques, exhibited superior performance compared to all pre-trained models. InceptionV3 closely trailed ResNet50 in terms of performance. However, the remaining pre-trained models showed suboptimal results, potentially due to overfitting concerns.

Model	**Accuracy**	**Loss**	**Accuracy**	**Loss**
CNN	0.74	0.58	0.93	0.28
VGG16	0.62	1.17	0.95	0.11
VGG19	0.67	0.63	0.49	0.69
RESNET50	0.72	0.86	0.97	0.12
INCEPTIONV3	0.67	1	0.94	0.12

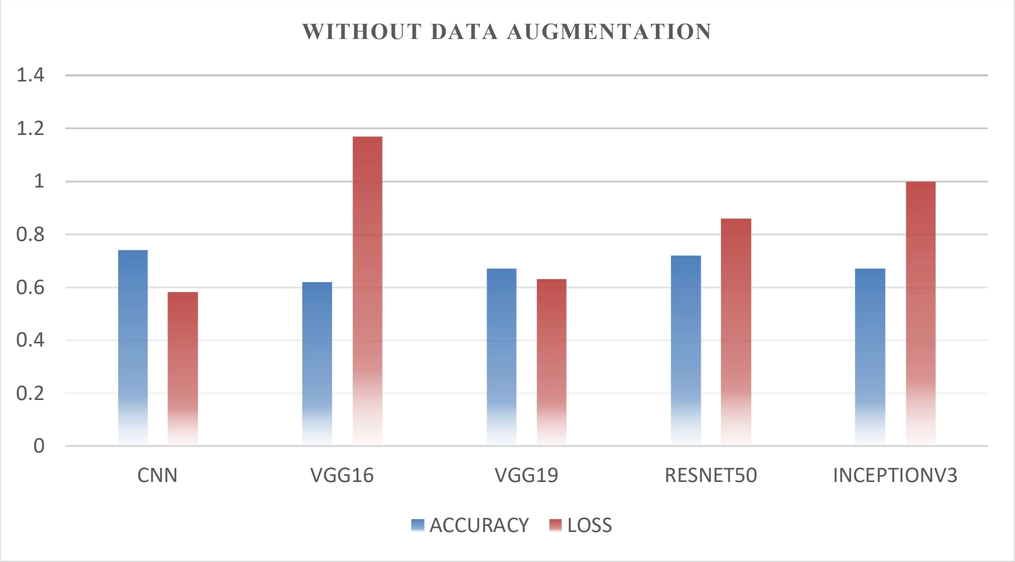


Fig 12. Comparison of Pre-trained model without Data augmentation

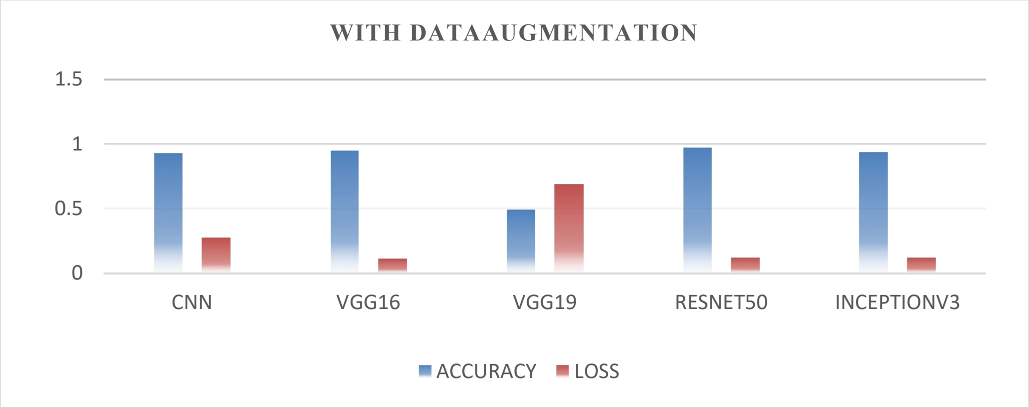


Fig 13. Comparison of Pre-trained model with Data Augmentation

5. Summary of Test Result

In this research paper, we conducted evaluations using Python, utilizing a Kaggle Notebook GPU cloud setup with a processing capacity of 2.30 GHz. The objective was to assess the proposed technique across three databases: Dredze, Image Spam Hunter (ISH), and an enhanced database.Table 2 presents a comprehensive summary of classification outcomes derived from five distinct deep learning models, integrating data augmentation, applied to the Dredze, ISH, and improved databases. It is evident that the integration of data augmentation leads to enhanced performance. Remarkably, the ResNet50 model consistently outperforms the others across all evaluation metrics for the three datasets. Furthermore, all models exhibit their best performance on the ISH dataset.Additionally, the average time taken for testing an input image and classifying it as either "ham" or "spam" is reported in Tables 3.To further analyze the results, Friedman's test procedure was applied to the datasets (Dredze, ISH, and improved) using the five pre-trained models. The results of Friedman's test are presented in Table 4. This test is a non-parametric method used to compare three or more related groups when the dependent variable is ordinal or ranked data.

Overall, the research findings suggest that the proposed technique, particularly when integrated with ResNet50 and data augmentation, yields promising results in the classification of image spam across diverse datasets.From the results presented in Tables 3, it is evident that ResNet50 and Inception consistently achieve the lowest rankings, indicating that they are the best performing classifiers. On the other hand, VGG16, CNN, and VGG19 have higher average rankings, suggesting that they are consistently the worst performing classifiers.Across all examined datasets, ResNet50 consistently attains the highest ranking in terms of validation accuracy. This indicates that ResNet50 outperforms other classifiers in accurately classifying spam images.Our proposed system demonstrates superior accuracy compared to other systems. Additionally, for the improved dataset, our most proficient model (ResNet50) surpasses alternative models in terms of accuracy, achieving an impressive 99% accuracy rate.These findings highlight the effectiveness of ResNet50 as a classifier for image spam detection, particularly when compared to other deep learning models such as VGG16, CNN, and VGG19.

Table 2. Comparison of three different dataset

Algorithm	ISH DATASET	DREEZE DATASET	IMPROVED DATASET	ISH DATASET
CNN	0.93	78	0.76	0.28
VGG16	0.95	82.6	97	0.11
VGG19	0.49	71.7	79	0.69
RESNET50	0.97	91	0.99	0.12
INCEPTIONV3	0.94	90	0.84	0.12

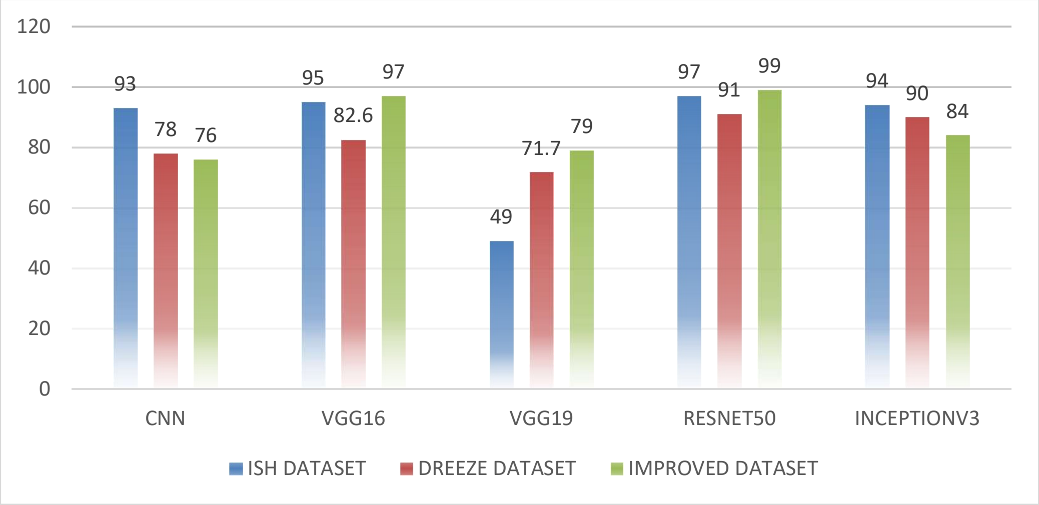


Fig 14. Comparison of three different dataset

Table 3. Computational testing time for the classification and Data Augmentation System measures in Seconds of 10 images

Algorithm	ISH DATASET	DREEZE DATASET	IMPROVED DATASET
CNN	3.08	1.08	2.09
VGG16	2.09	2.03	1.9
VGG19	1.6	1.8	1.9
RESNET50	1.005	1.007	1.008
INCEPTION V3	1.007	2.05	3.09

Table 4. Fried's man Test Result on Image Spam Hunter

CLASSIFIER	FRIEDMAN's TEST AVERAGING RANKING
CNN	3.667
VGG16	3.3
VGG19	4.67
RESNET50	1
INCEPTION	2.33

Table 5. PERFORMANCE OF STATE-OF-THE-ART IMAGE SPAM MODEL.

Reference	**Model**	**Dataset used**	**Accuracy**
PROPOSED WORK	RESNET50 WITH DATA AUGMENTATION	IMPROVED DATASET	99
[4]	DT classifier	UNINA dataset	97
[5]	RF classifier	http://www.seas.upenn.edu/ mdredze/datasets/imagespam.	96.8
[6]	CNN	ISH	96
[7]	SVM, CNN	ISH, dreeze dataset	98
[9]	SVM	ISH	97

6.Conclusions

This paper presents an innovative framework that utilizes multiple deep learning models, including InceptionV3, ResNet50, VGG16, and VGG19, to improve accuracy and reduce computational time in categorizing spam/ham images. The system's performance metrics focus on accuracy and computational efficiency. During the training process, the weights of a network pretrained on a different dataset are initialized, enhancing the generalization capacity of the pretrained network and mitigating overfitting. Results indicate that employing data augmentation positively impacts the performance of the classifiers, leading to improved outcomes. Notably, the study demonstrates that no human intervention, such as pre- or post-processing, or manual feature engineering, is necessary.Among the evaluated models, the ResNet50 Model, when coupled with Data Augmentation, achieves the highest performance on the Improved dataset, achieving an accuracy of 99%. Through comprehensive comparative analysis, it is evident that our proposed model, ResNet50 with data augmentation, outperforms other state-of-the-art techniques. Table 5 provides a performance comparison of our model with other state-of-the-art methods.

References

1. Symantec. (2019, November 8). Symantec monthly threat report. Retrieved from https://www.symantec.com/securitycenter/publications/monthlythreatreport#Spam

2. Krichen, M., Lahami, M., Cheikhrouhou, O., Alroobaea, R., & Maˆalej, A. J. (2020). Security testing of internet of things for smart city applications: A formal approach. In Smart Infrastructure and Applications (pp. 629–653). Springer, Cham.

3. Akarsh, S., Sriram, S., Poornachandran, P., Menon, V. K., & Soman, K. (2019). Deep learning framework for domain generation algorithms prediction using long short-term memory. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 666–671). IEEE.

4. Gargiulo, F., & Sansone, C. (2008). Visual and OCR-Based Features for Detecting Image Spam. In PRIS (pp. 154-163).

5. Shen, J., Deng, R. H., Cheng, Z., Nie, L., & Yan, S. (2015). On robust image spam filtering via comprehensive visual modeling. Pattern Recognition, 48(10), 3227-3238.

6. Makkar, A., & Kumar, N. (2021). Protector", An optimized deep learning-based framework for image spam detection and prevention. Future Generation Computer Systems, 125, 41-58.

7. Sharmin, T., Di Troia, F., Potika, K., & Stamp, M. (2020). Convolutional neural networks for image spam detection. Information Security Journal: A Global Perspective, 29(10), 1–15.

8. Nam, S-G., Jang, Y., Lee, D-G., & Seo, Y-S. (2022). Hybrid Features by Combining Visual and Text Information to Improve Spam Filtering Performance. Electronics, 11(13), 2053.

9. Kumaresan, T., Saravanakumar, S., & Balamurugan, R. (2019). Visual and textual features based email spam classification using S-Cuckoo search and hybrid kernel support vector machine. Cluster Computing, 22(1), 33–46.

10. Hayati, P., & Potdar, V. (2008, November). Evaluation of spam detection and prevention frameworks for email and image spam: a state of art. In Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services (pp. 520-527).

11. Makkar, A., & Kumar, N. (2021). PROTECTOR: An optimized deep learning-based framework for image spam detection and prevention. Future Generation Computer Systems, 125, 41-58.

12. Kim, B., Abuadbba, S., & Kim, H. (2020). DeepCapture: image spam detection using deep learning and data augmentation. In Information Security and Privacy: 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30–December 2, 2020, Proceedings 25 (pp. 461-475). Springer International Publishing.

13. Annadatha, A., & Stamp, M. (2018). Image spam analysis and detection. Journal of Computer Virology and Hacking Techniques, 14, 39-52.

14. Su, C. Y., Shen, D. F., & Lin, G. S. (2017, June). An image spam detection method. In 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW) (pp. 71-72). IEEE.

15. Fatichah, C., Lazuardi, W. F., Navastara, D. A., Suciati, N., & Munif, A. (2019). Image spam detection on instagram using convolutional neural network. In Intelligent and Interactive Computing: Proceedings of IIC 2018 (pp. 295-303). Springer Singapore.

16. Raju, R. K., & Lakshmi, V. A NOVEL IMPLEMENTATION OF PEDESTRAIN DETECTION USING HOGD AND SVM ALGORITHMS. The Journal of Computational Science and Engineering, 1(2), 1-7.

17. Ammar, M. H., & Zegura, E. W. (2009). Introduction to Delay-Tolerant Networking and Its Application to Space Missions. IEEE Journal on Selected Areas in Communications, 27(5), 553–561.

18.Shankar, K., Reddy, K. S., Babu, D. A., & Aswin, B. Transforming Industries and Innovating Design-3D Printing. The Journal of Computational Science and Engineering, 1(4), 1-9.

19. Amir, A., Srinivasan, B., & Khan, A. I. (2018). Distributed classification for image spam detection. Multimedia Tools and Applications, 77, 13249-13278.

20. Das, M., & Prasad, V. (2014). Analysis of an image spam in email based on content analysis. International Journal on Natural Language Computing (IJNLC), 3(3), 129-140.

21. Shen, J., Deng, R. H., Cheng, Z., Nie, L., & Yan, S. (2015). On robust image spam filtering via comprehensive visual modeling. Pattern Recognition, 48(10), 3227-3238.

22. Zhang, Y., Wang, S., Phillips, P., & Ji, G. (2014). Binary PSO with mutation operator for feature selection using decision tree applied to spam detection. Knowledge-Based Systems, 64, 22-31.

23. Kumaresan, T., Sanjushree, S., & Palanisamy, C. (2015). Image spam detection using color features and K-Nearest neighbor classification. International Journal of Computer and Information Engineering, 8(10), 1904-1907.

24. Annareddy, S., & Tammina, S. (2019, December). A comparative study of deep learning methods for spam detection. In 2019 third international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 66-72). IEEE.

25. Belkhouche, Y. (2022, September). A language processing-free unified spam detection framework using byte histograms and deep learning. In 2022 Fourth International Conference on Transdisciplinary AI (TransAI) (pp. 83-86). IEEE.

26. Wan, P., & Uehara, M. (2012, March). Spam detection using Sobel operators and OCR. In 2012 26th International Conference on Advanced Information Networking and Applications Workshops (pp. 1017-1022). IEEE.

27. Hsia, J. H., & Chen, M. S. (2009, June). Language-model-based detection cascade for efficient classification of image-based spam e-mail. In 2009 IEEE International Conference on Multimedia and Expo (pp. 1182-1185). IEEE.

28. Rathod, S. B., & Pattewar, T. M. (2015, April). Content based spam detection in email using Bayesian classifier. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1257-1261). IEEE.

29. Mohammed, M. A., Mostafa, S. A., Obaid, O. I., Zeebaree, S. R., Abd Ghani, M. K., Mustapha, A., ... & AL-Dhief, F. T. (2019). An anti-spam detection model for emails of multi-natural language. Journal of Southwest Jiaotong University, 54(3).