iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63490

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Images Spam Detection on Online Social Media using CNN with Pre-Trained Model

Himani Jain[1], Amit Dixit[2]
[1]*Quantum University, Roorkee, Uttarakhand Ph.D. Scholar, India*
[2]*Dean Research Quantum University, Roorkee, Uttarakhand, India*

Abstract: ***Nowadays attackers move to image spam techniques instead of text based. The Majority of conventional techniques solely possess the capability to identify spam confined to textual content and hyperlinks. In this research we have done "Deep Convolutional Neural Networks" (DCNNs)in conjunction with pre-trained architectures. Image classification is one of the areas that has increased in the last decade very rapidly. But due to the less computational resources it become very challenging to train a good image classification model. With the help of Transfer learning, we can overcome this type of situation and can build a good image classification model. Our proposed model utilizes deep convolutional neural networks (DCNNs) along with pre-trained architectures. By fine-tuning this pre-trained model on the specific image dataset, the model can effectively learn to detect image- based spam content. Our suggested model surpasses contemporary state-of-the-art detection models concerning both accuracy and efficiency in the realm of the image spam identification.***

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

I. INTRODUCTION

The Internet has become popular nowadays due to cost effective techniques. Due to low cost, great efficiency, mostly people start using online social sites. Many users use online communities for various activities. Online communities have become hubs for diverse activities[34]. With the desire for popularity driving them, many individuals are drawn to join these social sites, often unaware of the potential criminal activities, that occur within the realm of social media. Nowadays everybody wants to join social sites to become popular. But some of them are not aware that criminal activities are happening on social media. The attackers are always attracting users so that they fall into their trap. In the past, spam predominantly took the form of text-based content. However, contemporary spammers have evolved their tactics, resorting to the utilization of images to capture's user attention and convey their intended messages. Spammers send the images in various forms like Product or services promotion's form, Fake giveaways or contests, Phishing Scams, Malware distribution. In product or services promotions spammers send the illegal and counterfeit products. These types of images contain user information. In Fake giveaways and contents spammers send the images that content fake prices, offers and exclusive offers to get the users attention. In Phishing scams spammers create visually convincing posts or messages that resemble legitimate companies or website. In Malware distribution spammers send the images that contain malware. Attackers may embed malicious code or links within the images [1]. Traditionally, machine learning techniques have been developed to combat text-based spam, including "support vector machine, K-Nearest Neighbours, Naïve Bayes" algorithms etc. However, as attackers constantly adapt, they have introduced image spam as a new method to deceive users. Various approaches to detecting image spam have emerged. Initially optical character recognition (OCR) techniques were employed. Followed by the development of deep learning-based methods [2]. The depth of deep learning model promises enhanced classification reliability and accuracy through automated features extraction, unsupervised features learning, and pattern recognition. Deep learning model encompass convolutional and pooling layers, enabling efficient features selection and extraction. It is a relatively new form of image spam detection because in deep learning several layers give the hope to build a more reliable classifier with high accuracy, where numbers of layers of data make the model more reliable. It is a time-consuming features selection and extraction process. It contains two types of layers one is convolutional layers and other is pooling layers [3]. The convolutional layers include multiple filter and pooling layers using various methods to reduce the size. A "Transfer learning" is a tool that employs a "pre-trained model" instead of construction a model from scratch. "Transfer learning" decreases the computational cost that is needed in deep learning models. This paper's core focus lies in classifying images into ham and spam categories.

©IJRASET: All Rights are Reserved

To achieve this various deep learning model are explored, with the transfer learning approach employed to minimize training time and computational demands. The contribution of this study is multifold. Transfer learning is leverage to optimize model development efficiency by conserving training time and computational resources. Performance comparison are conducted across different pre-trained deep learning models "VGG16, VGG19, Resnet50, Inception V3" for image spam detection. Multiple datasets including "Image spam Hunter dataset, Dredze dataset, and an Improved dataset" are utilized Novel CNN-based techniques are devised to achieve high accuracy image spam detection beyond the current "state-of-the-art".

The primary division of this work as follows.

1) "DCNN" models for image spam detection utilizing diverse datasets are developed.
2) "Transfer learning" techniques employing pre-trained models are implemented to enhance effectiveness.
3) Dataset descriptions are provided.
4) Methodology and implementation details are elaborated.
5) Result and conclusions are presented, highlighted the significance of the research.

While extensive research has historically focus on text, links and emails spam, the realm of image spam detection remains relatively underexplored. Figure 1 show some spam images.



Fig 1. Sample Spam images

II. LITERATURE SURVEY

Various researchers have made significant contributions to the filed of image spam detection through the exploration of different techniques and datasets. Here are summaries of some of their finding.

F. Gargiulo and C. Sansone (2008) [4] used two set of features to identify spam images from UNINA and DREDZE datasets. Their approach involved employing visual features and OCR -Based features feeding them into decision tree. which achieved an accuracy. UNINA dataset Accuracy of Visual features is 94.31 and OCR 94.79%. And proposed approach accuracy is 97% and F1 Score is 0.97.

Shen et al. (2015) [5] constructed a novel system called RoBoTs based on an efficient learning sample selection scheme and ensemble method with the help of random forest and linear discriminative analysis. They used three datasets. An accuracy of 96.8%was achieved for the Dredze dataset.

Makkar et al. (2021) [6] constructed an optimized framework called PROTECTOR. They provide the rank score to each image. An images filtering scheme is proposed to analyse the features of images and detect the spam images with the help of rank score. They used image spam hunter dataset and having an accuracy of 96%.

Sharmin et al (2020) [7] used CNN to detect image spam techniques. They used ISH dataset, Challenge datset1 and Challenge dataset2. They used SVM and two neural networks-based techniques, Multilayers perceptron's and CNN. They experimented with features based on raw images, Canny images and novel combination of the two. CNN perform better than SVM having an accuracy of 99.02%.

Guk Nam et al [8] employed a blend of textual and visual data to enhance the efficiency of image spam filtering. They synergistically harnessed optical character recognition, latent Dirichlet allocation, and word2Vec methodologies for features extraction from images, resulting in an impressive accuracy of 0.9814.

Kumaresan et al [9] employed an S-Cuckoo spam classification framework in conjunction with hybrid kernel-based support vector machine (HKSVM). The approach involved extracting features from emails, encompassing both textual and image base components. Their efforts culminated in achieving an impressive accuracy level of 97.235%

These studies collectively showcase diverse methodologies for detecting image spam ranging from features -based approaches to the applications of deep learning techniques, all contributions to enhancing the accuracy and efficiency of "image spam detection" systems.

III. METHODOLOGY

A. *Pre-processing*

In our work we have used three datasets but in all three dataset many corrupt and duplicate files are found. To address this challenge, we leveraged the concept of hashing. this involved generating unique hash value for each image and subsequently identifying instance where multiple images shared the same hash value. In such case, we opted to exclude the redundant images. Following the duplication process, we focused on ensuring a consistent and standardized dataset. To achieve this, all the remaining unique images underwent a twostep process : normalization and resizing. This procedure aimed to establish a uniform appearance for the images while achieving the desired dimensions. Our proposed framework is illustrated in Figure 2.

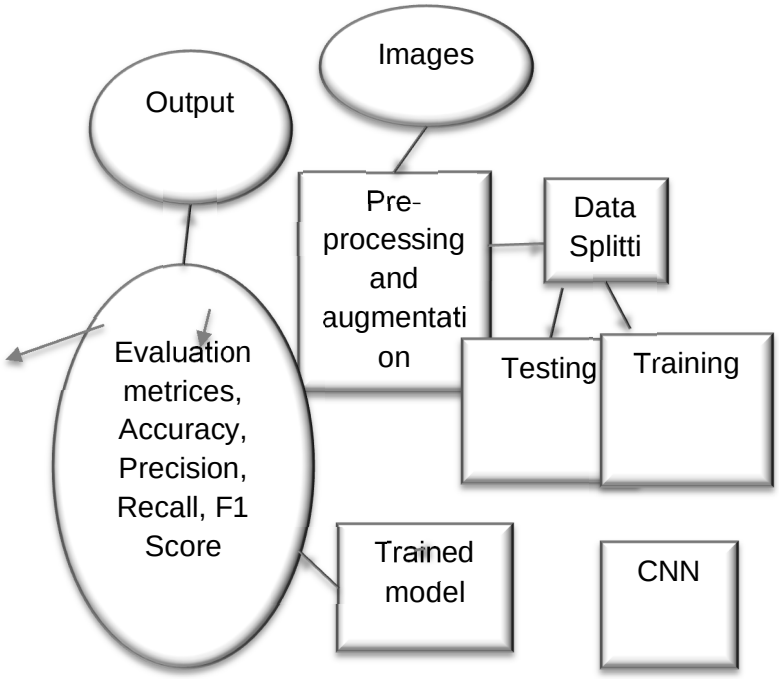


Fig. 2 Proposed Framework for Image Spam Filtering.

B. *Datasets and Data Augmentation*

The following dataset we have used in our work.

1) "Image spam hunter dataset" (ISH)

This dataset is publicly available which contains both ham and spam images. It can be found on the North-western University website [31]. There are a total of 810 ham and 929 spam images. There are some duplicate images found in this dataset so duplicate images are deleted out of which 879 ham images are found uniquely and 810 spam images are found.

2) "Improved Images Dataset"

This dataset contains a total 1029 spam images. but the unique image is 975. This dataset is used to improve the 'performance of image spam models' with more advanced images spam [32].

3) "Dredze Image Spam Dataset"

The dataset referenced as [33] comprises three distinct sets of images, each serving a specific purpose. The first set, labeled as Personal Ham (PHam), encompasses a total of 2,021 images. Among these, 1,517 images are unique and distinct from one another. The second set, designated as Personal Spam (PSpam), encompasses a larger collection of 3,298 images. Within this set, 1,274 images are unique and do not duplicate across the dataset. Lastly, the third set, referred to as Spam Archive (SpamArch), is notably extensive with a total of 16,028 files. These files encompass a variety of formats including JPEG, PNG, GIF, among others. Among the diverse files, there are 3,039 unique images that distinguish themselves within the dataset.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Convolutional Neural Network

In this research paper, we have employed "Convolutional Neural Networks" (CNNs) for the purpose of image classification tasks, utilizing the Keras API with the TensorFlow backend. Our network architecture consists of multiple layers that contribute to the overall classification process.

First Layer (Convolutional Layer): We initiated our model with 8 filters of varying sizes, applying activation using the "Rectified Linear Unit" (ReLU) function. The ReLU function is applied element-wise, replacing negative values with zero, which introduces non-linearity to the network.

Second Layer (Max Pooling): Subsequently, a max pooling layer with a pool size of (2,2) was incorporated. This operation reduces the spatial dimensions (width and height) of the output from the previous layers by a factor of 2, achieved by selecting the maximum value within each 2x2 region.

Third Layer (Convolutional Layer): The following layer involved the use of 16 filters of size (3,3), applying the same ReLU activation function and padding strategy as in the first layer.

Fourth Layer (Max Pooling): Another "max pooling layer" with a pool size of (2,2) followed, further reducing spatial dimensions.

Fifth Layer (Convolutional Layer): For this layer, we utilized 32 filters of size (3,3), followed by activation and padding.

Sixth Layer (Max Pooling): Subsequent to the fifth layer, another max pooling operation was employed.

Seventh Layer (Convolutional Layer): In this layer, we adopted 64 filters.

Eighth Layer (Max Pooling): Following the seventh layer, another max pooling layer was included.

Ninth Layer (Flatten Layer): The output from the previous layers was flattened into a vector, preparing it for connection to fully connected layers.

Tenth Layer (Dense Layer): This layer was designed with 512 units and applied the ReLU activation function.

Eleventh Layer (Fully Connected Layer): The penultimate layer consisted of a single unit, utilizing the "sigmoid activation" function. This function yields output probabilities in the range of 0 to 1, appropriate for binary classification tasks.

For optimization, we employed the 'Adam optimizer' with a learning rate set at '0.001'. To measure the loss and guide the training process for binary classification, we employed the binary cross-entropy loss function.

This architectural setup reflects our approach to leveraging CNNs for image classification tasks within the specified framework. In this paper A sequential 4-layer CNN model was built, trained and validated on the two-class "Image spam hunter dataset". The average training time for one epoch took 15 min on an Intel(R) Core (TM) i3-7020U CPU @ 2.30GHz with 8GB RAM. Hence, only five epochs were performed. In Figure 3 CNN with 4- layers with accuracy and Loss are shown.

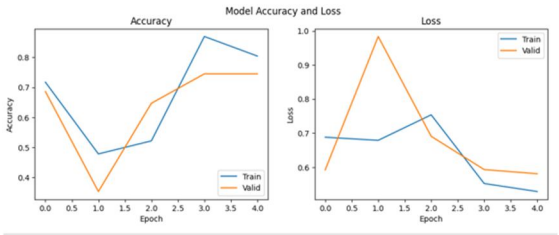


Fig3 CNN with 4 layers

D. Transfer Learning

'Transfer learning' is a "machine learning technique" that reuses a pretrained model instead of a new model. It is used to gain knowledge from solving one problem and apply it into another problem. It is very fast because the model is already learned to recognize the relevant features in the data. We used Pretrained model and weight architecture to solve our problem. In this paper we have used pretrained weights of VGG16, VGG19, Resnet50, InceptionV3.

1) VGG16

The VGG16 architecture is characterized by its deep structure consisting of 16 layers, which include 'convolutional layers' followed by fully connected layers. The key features of the VGG16 architecture are as follows:

Architecture Depth: VGG16 comprises a sequence of convolutional layers, with a total of 13 convolutional layers (including five max-pooling layers) followed by three fully connected layers.

Convolutional Layers: The convolutional layers use small (3x3) filters with a stride of 1 and a fixed padding size of 1. The use of multiple stacked convolutional layers helps the network learn increasingly complex and abstract features.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Max-Pooling Layers: Max-pooling layers with a pool size of (2,2) are employed to down sample the spatial dimensions of the feature maps, which helps in reducing computation and controlling overfitting.
Fully Connected Layers: The final layers of the network are fully connected layers that are responsible for making predictions based on the learned features from the previous layers.
Activation Function: The ReLU (Rectified Linear Unit) activation function is used after each convolutional and fully connected layer, introducing non-linearity to the network.
Output Layer: The output layer typically consists of SoftMax activation for multiclass classification tasks, yielding class probabilities. Figure 4 visually displayed metrics related to accuracy and loss.

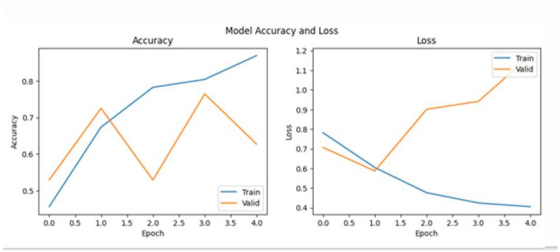


Fig 4. VGG16 pre-trained model

2) VGG19

"VGG19 represents a deep neural network architecture featuring 19 layers, which comprises 16 convolutional layers and 3 fully connected layers". It was subjected to training on an extensive ImageNet dataset, intended for the purpose of image classification. The study employed matrices of images with dimensions 128 by 128 and a color depth of 3.
The convolutional layers utilized kernels of size 3 by 3, adopting a stride of 1 pixel. Employing spatial padding was essential to maintain the original spatial dimensions of the input images. Furthermore, a 2 by 2 max pooling approach was employed with a stride of 2 pixels to down sample the data. Incorporating Rectified Linear Units (ReLU) activation function enhanced both model performance and computational efficiency.Visual representations were provided to illustrate the architecture of VGG as depicted in Figure 5, whereas Figure 6 visually displayed metrics related to accuracy and loss.

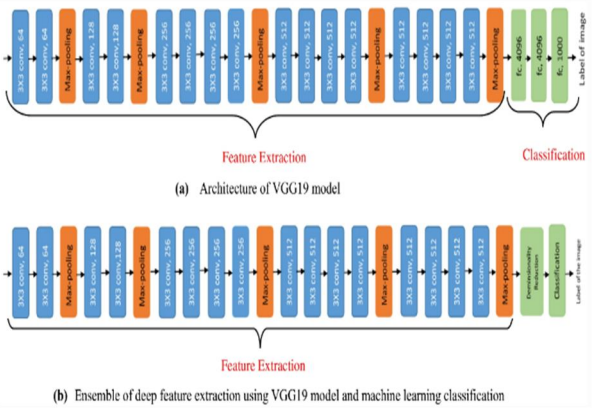


Fig 5. VGG19 architecture

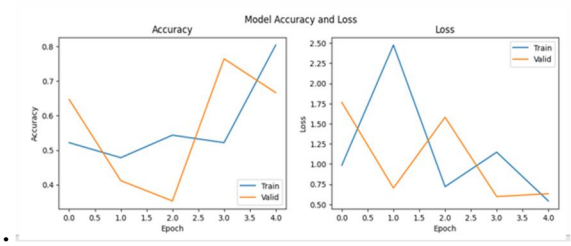


Fig 6. VGG19 Accuracy and loss

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.

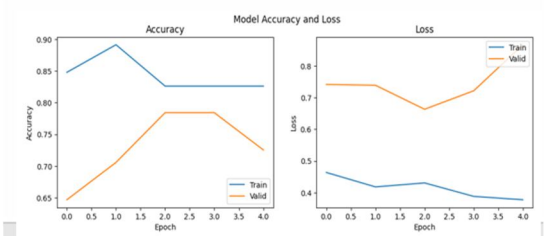


Fig 7. Resnet50 Accuracy and loss

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.

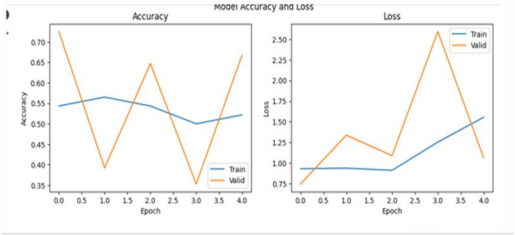


Fig 8. Inceptionv3 Accuracy and loss

E. Data Augmentation

“Data Augmentation” technique is used to surge the size and diversity of training dataset. It is used for transformation or modification to existing data samples, resulting in new dataset and slightly alternation version of original dataset. The Objective of Data Augmentation is used to create additional training samples that capture the same underlying patterns and concepts but with slightly variations of original dataset. So that our model can become more robust and generalizes better to unseen data during training. In our paper we have used various augmentation in our dataset like flipping horizontal or vertical, rotation, Translation, Scaling, Cropping, Shearing, Addition noise, changing brightness, contrast or Saturation The impact of these augmentation strategies on the performance of diverse transfer learning models has been documented in Figures 9, 10, 11,12 and 13. These figures present a visual depiction of how data augmentation influences accuracy and loss metrics within the context of various transfer learning models.

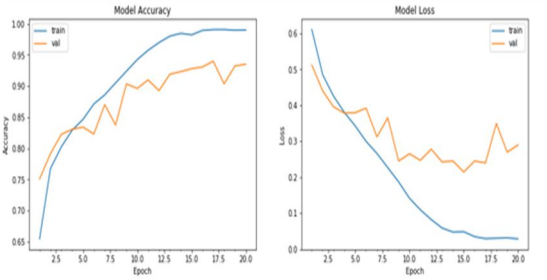


Fig 9. CNN After Data Augmentation

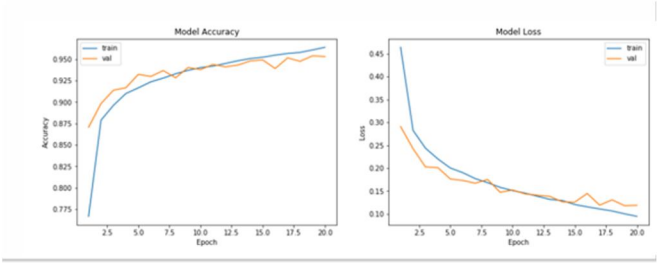


Fig 10. VGG16 After Data Augmentation

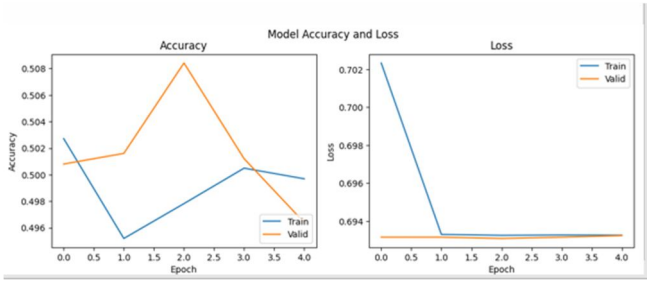


Fig 11. VGG19 After Data Augmentation

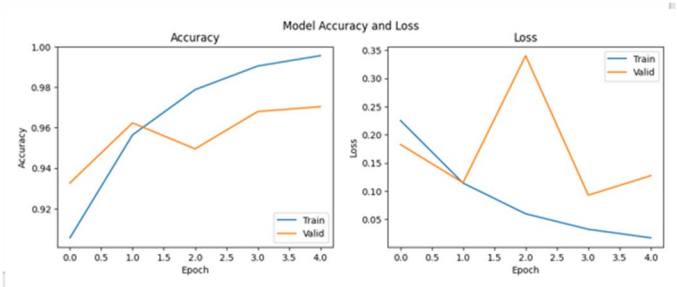


Fig 12. Resnet50 After Data Augmentation

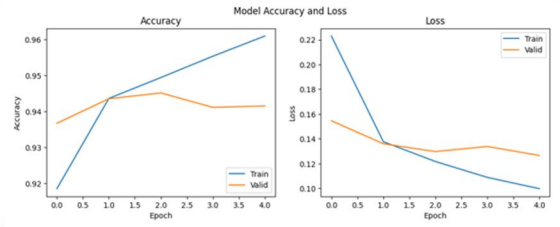


Fig 13. IneptionV3 After Data Augmentation

IV. EXPERIMENTAL RESULT AND DISCUSSION

In this paper we used many trainings model like VGG16, VGG19, Inception, Resnet50. We used the Google Colab to implement our proposed model. This study involves the implementation of our proposed models using the Kera's and Scikit-learn Python libraries. To optimize the learning process, we employ the "binary cross-entropy" loss function along with the "Adam optimizer". In order to prevent overfitting, dropout regularization is incorporated. The dataset employed in this study has been partitioned into a ration of 70:30 ,with 70% for training and the remaining 30% reserved for testing objectives. The CNN1 and CNN2 models are trained using images resized to a resolution of 128x128 pixels, a size determined through experimentation across various input dimensions. Our proposed models are trained and evaluated using 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 (Performance of model with and without Data Augmentation. (Image Spam Hunter Dataset).

Our proposed models consistently outperform existing ones. Moving on, pre-trained architectures listed in Figure 14 and Figure 15 are show the graphical representation of table1. With images resized to a resolution of 128x128 pixels, the performance metrics indicate that Resnet50 outperforms other models. Our proposed "Resnet50 model", augmented with data augmentation techniques, showcases superior performance in comparison to all pre-trained models. The InceptionV3 model closely trails Resnet50 in terms of performance.

The remaining pre-trained models exhibit suboptimal results, potentially due to overfitting concerns.

Table 1

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

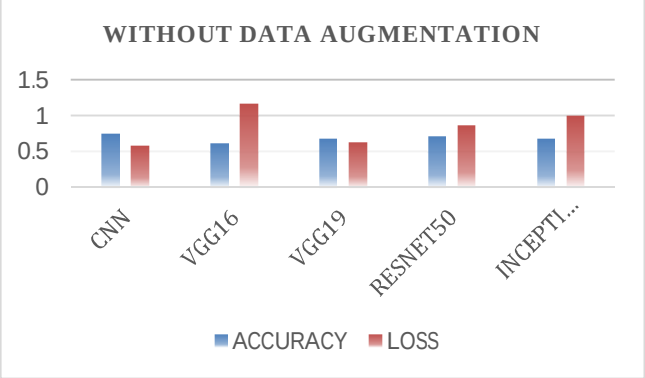


Fig 14. Comparison of Pre-trained model without Data augmentation

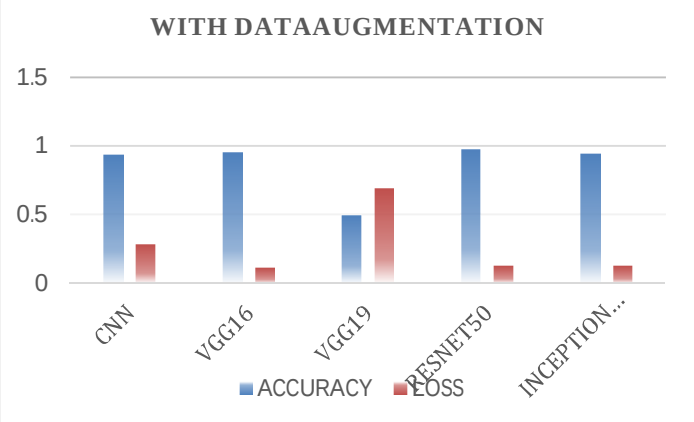


Fig 15. Comparison of Pre-trained model with Data Augmentation

V. SUMMARY OF TEST RESULT

In this research paper, we conducted evaluations using the Python utilizing a Kaggle Notebook GPU cloud setup 2.30 GHz processing capacity. 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. Evidently, the integration of data augmentation leads to enhanced performance. Remarkably, the ResNet50 model consistently outperforms the others across all evaluation metrics for the 3 datasets. Furthermore, all models exhibit their best performance on the "ISH dataset". Notably, the average time taken for testing an input image and classifying it as either "ham" or "spam" is reported in Tables 3. Friedman's test procedure was applied to the datasets (Dredze, ISH, and improved) using the five pre-trained models, we applied Friedman's test result on three different datasets in Table 4. It is a non -parametric method to compare three or more related groups when the dependent variable is ordinal or ranked data.

$$R_{J=\frac{1}{N}}\Sigma_i r_{ji} \quad (1)$$

We can see that RESNET50 and INCEPTION have the lowest rankings, so they are the best performing classifiers, while VGG16, CNN, VGG19 has the higher average ranking which seems to indicate that it's consistently the worst performing classifier. The outcomes are depicted in Tables 3. Across all examined datasets, ResNet50 consistently attains the highest ranking in terms of validation accuracy. Evidently, our proposed system demonstrates superior accuracy compared to other systems. Furthermore, for the improved dataset, our most proficient model (ResNet50) surpasses alternative models in terms of accuracy, achieving an impressive 99% accuracy rate.

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

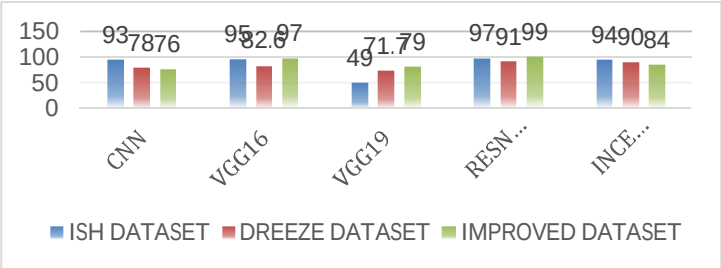


Fig 16. Comparison of three different dataset

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
INCEPTIONV3	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

VI. CONCLUSIONS

This paper introduces an innovative framework that leverages multiple "deep learning models", namely "InceptionV3, ResNet50, VGG16, and VGG19", to enhance the accuracy and minimize computational time in the task of categorizing spam/ham images. The system's performance metrics encompass accuracy and computational efficiency. The training process involves initializing the weights of a network pretrained on a distinct dataset. This augmentation enhances the generalization capacity of the pretrained network, thereby mitigating overfitting. The results indicate that employing data augmentation positively impacts the performance of the analysed classifiers, leading to enhanced outcomes. One significant aspect of this study is its demonstration that no human intervention, such as pre- or post-processing, or manual feature engineering, is necessary. Among the models evaluated, "ResNet50 Model", coupled with "Data Augmentation", attains the highest performance on the Improved dataset, achieving an accuracy of 99%. Through a comprehensive comparative analysis, it becomes evident that our proposed model, ResNet50 with data augmentation, outperforms other state-of-the-art techniques. Table 5 shows the performance and comparison of our model with other state-of-the-art.

Table 5. Performance of State-OF-THE-ART Image Spam Model.

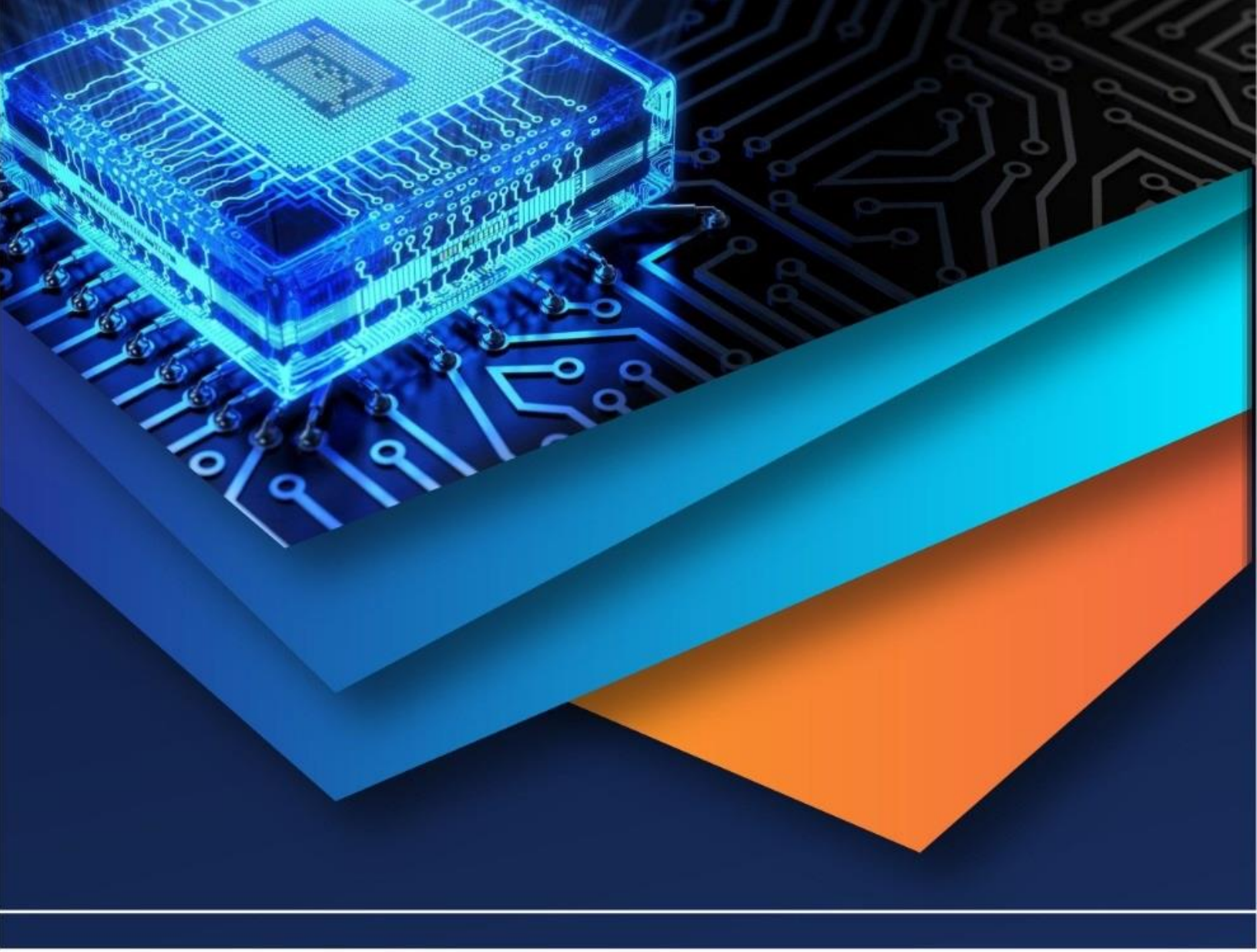
Reference	Model	Dataset used	Accuracy
PROPOSED WORK	RESNET 50 WITH DATA AUGMENTATION	IMPROVED DATASET	99
[4]	DT classifier	UNINA dataset	97
[5]	RF classifier	http://www.seas.upenn.edu/mdredze/datasets/imagespam.	96.8
[6]	CNN	ISH	96
[7]	SVM, CNN	ISH, dreeze dataset	98
[9]	SVM	ISH	97

REFERENCES

[1] "Symantec monthly threat report," accessed: 08 Nov 2019. [Online]. Available: https://www.symantec.com/securitycenter/publications/monthlythreatreport#Spam.
[2] M. Krichen, M. Lahami, O. Cheikhrouhou, R. Alroobaea, and A. J. Maˆalej, "Security testing of internet of things for smart city applications:A formal approach," in Smart Infrastructure and Applications. Springer,Cham, 2020, pp. 629–653.
[3] S. Akarsh, S. Sriram, P. Poornachandran, V. K. Menon, and K. Soman,"Deep learning framework for domain generation algorithms predictionusing long short-term memory," in 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). IEEE,2019, pp. 666–671.
[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] A. Makkar, N. Kumar, Protector", An optimized deep learningbased framework for image spam detection and prevention",Futur. Gener. Comput. Syst. (2021).
[7] T. Sharmin, F. Di Troia, K. Potika, M. Stamp, Convolutional neural networks for image spam detection, Informat. Security J.Global Perspective 29 (10) (2020) 1–15.
[8] Nam S-G, Jang Y, Lee D-G, Seo Y-S. Hybrid Features by Combining Visual and Text Information to Improve Spam Filtering Performance. Electronics. 2022; 11(13):2053. https://doi.org/10.3390/electronics11132053.
[9] T. Kumaresan, S. Saravanakumar, R. Balamurugan, Visual and textual features based email spam classification using S-Cuckoo search and hybrid kernel support vector machine, Clust.Comput. 22 (1) (2019) 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] Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: challenges, open issues, and future directions. Expert Systems with Applications, 186, 115742.
[17] Shao, Y., Trovati, M., Shi, Q., Angelopoulou, O., Asimakopoulou, E., & Bessis, N. (2017). A hybrid spam detection method based on unstructured datasets. Soft Computing, 21, 233-243.
[18] Kumar, A. D., & KP, S. (2018). Deepimagespam: Deep learning based image spam detection. arXiv preprint arXiv:1810.03977.
[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).
[30] Jain, G., Sharma, M., & Agarwal, B. (2019). Optimizing semantic LSTM for spam detection. International Journal of Information Technology, 11, 239-250.
[31] Y. Gao, M. Yang, X. Zhao, B. Pardo, Y.Wu, T. N. Pappas, and A. Choudhary, "Image spam hunter," in 2008 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2008, pp. 1765–1768.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[32] A. Annadatha, "Improved spam image dataset,"accessed: 12 Sep 2019. [Online]. Available:https://www.dropbox.com/s/7zh7r9dopuh554e/New Spam.zip?dl=0
[33] M. Dredze, "Image spam dataset 2007," accessed: 12 Sep 2019. [Online].Available: http://www.cs.jhu.edu/ mdredze/datasets/image spam/
[34] K. Tzovelekis, V. Kanakaris and D. V. Bandekas(2018).," Geo-Location Twitter And Instagram Based On OSINT Techniques: A Case Study" February 2018International Journal of Advanced Research DOI: 10.21474/IJAR01/6283



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)