IDENTIFICATION OF IMAGE SPAM USING DEEP LEARNING TECHNIQUES

Anju Ajeendran M[1], Beena S[2]

[1]M. Tech Student, Dept. of ECE, Government Engineering College, Kerala, India
[2]Assistant Professor, Dept. of ECE, Government Engineering College, Kerala, India

---***---

Abstract – *With the colossal growth of the internet, many people are contingent on it for their social interactions, communications and financial transactions. Cyberspace is facing several threats from the attackers and threats like spam e-mails account for 75% of total e-mails according to Symantec monthly threat report. Gradually, attackers advances onto image spam to evade text-based spam filters. Hackers and spammers intentionally fool peoples by innovative and novel techniques to deceive novice and knowledgeable or even educated internet users. Image spam attack necessitate the images with text embedded to it and hence spammers changes some portion of the image which is indistinguishable from the original image thereby fooling the users. To tackle with this, researchers came up with several machine learning and deep learning approaches that depends on features. But, the Deep Convolutional Neural Network models, transfer learning and cost- sensitive learning-based approaches are not scrutinized much for image spam detection. Convolutional Neural Network method avoids manual feature extraction task by automatically identifying the features by itself thus reducing time and effort. In this work, two deep learning models along with pretrained ImageNet architecture like VGG19 are trained on combined datasets and utilization of hybrid model with the developed CNN network on various ML classifiers are also employed. Comparison of cost-sensitive and cost-insensitive learning approach to handle data imbalance on various ML classifiers are studied with the latter CNN network. Some of the proposed models in this work attained an accuracy of 98.6% with low false positive rate in best case.*

Key Words: Image spam, spammers, Deep learning, Spam detection, Convolutional Neural Network, Cost-sensitive learning, Transfer learning, etc

1. INTRODUCTION

Internet has become a requisite part for majority of the people today and many of our financial transactions, social dealings and communications are principally dependent on it and may not always completely safe. Intruders, hackers and attackers are always in the quest for exploiting the users by hacking, spamming etc. In recent years, the key public cost-effective and embattled attack is the sending of spam to users. According to the report released by Symantec, email spam accounted for approximately 70% of emails in mining, finance, insurance, real estate industries and techniques like spam filters are essential for safe and secure email communication. Internet of Things (IOT) technologies are growing very swiftly and the disadvantage is that they are low powered devices with limited resources and are not built with security in mind. Several hackers are abusing the IoT Bot network (the network of compromised IoT devices) for directing various cyber-attacks. An overwhelming 17 million Americans faced the identity theft in 2017, according to Javelin strategy. Cybercriminals use malware, spyware and phishing techniques to break into the online accounts or device and steal some personal information to engage in activities like identity theft. Spam in its inceptive period was only in the form of texts. With the beginning of machine learning, many classifiers were advanced to filter such spam based on email content. Several ML based recognition techniques are used to filter spam e-mails and for sorting purposes. Later on, spammers came up with innovative notions to fool content created classification techniques. Thus, image spam was established, where undesirable textual information was distributed in the form of images. Image spam attack comprises images with text inserted into it and they are used by invaders to escape from text-based spam filters. These images usually ruse the user to click on it which might cause redirection to unsafe websites and may causes malware infection. Day by day, they are getting fruitful experiences in convincing people to respond to these bogus offers, thus both educated and uneducated people are smoothly getting trapped of it.

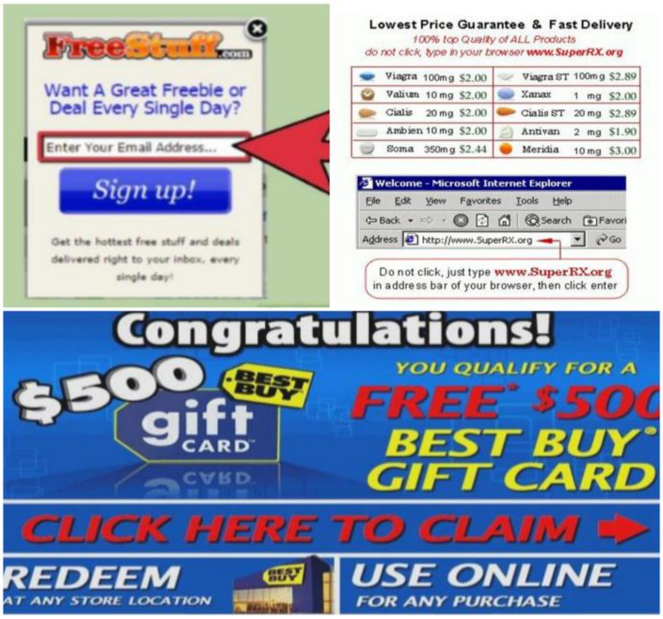

FreeStuff.com
Want A Great Freebie or Deal Every Single Day?
Enter Your Email Address...
Sign up!
Get the hottest free stuff and deals delivered right to your inbox, every single day!
Lowest Price Guarantee & Fast Delivery
100% top Quality of ALL Products
do not click, type in your browser www.SuperRX.org
Viagra 100mg $2.00
Viagra ST 100mg $2.89
Valium 10 mg $2.00
Xanax 1 mg $2.00
Cialis 20 mg $2.00
Cialis ST 20 mg $2.89
Ambien 10 mg $2.00
Antivan 2 mg $1.90
Soma 350mg $2.44
Meridia 10 mg $3.00
Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favori
Address http://www.SuperRX.org Go
Do not click, just type www.SuperRX.org in address bar of your browser, then click enter
Congratulations!
$500 gift CARD
BEST BUY
YOU QUALIFY FOR A
FREE* $500
BEST BUY GIFT CARD
CLICK HERE TO CLAIM
REDEEM AT ANY STORE LOCATION
USE ONLINE FOR ANY PURCHASE

Fig -1: Sample spam images

1.1 Research Background

Textual content-based image spam detection is formed primarily. Optical character recognition (OCR) techniques [1] were used to extract text from images, which is then analyzed by various text filters to detect spam. But spammers have applied several image processing methods like varying foreground, background, text, font, size and color, thus OCR techniques became less effective. Also, spammers started using obfuscation techniques, so OCR techniques became less used one. A Probabilistic Boosting Tree (PBT) classifier based spam detection model is proposed in [2]. It is used to give soft decision on whether an incoming image is spam or not. Based on efficient global image features i.e., color and gradient orientation histograms are extracted and fed into the classifier. In [3] two solutions were proposed for detecting spam images. The first solution consists of using an SVM to classify images. The second solution consists of using Gaussian mixture models to detect similar images, in a probabilistic manner. Thus, the authors start from the assumption that a spam image may belong to a cluster of images with similar features. The rates of correct image classification in the studies ranges from 89% to 92.6%. [4] proposed an architecture based on Neural networks and Back Propagation Neural Networks (BPNN) for image spam detection. They achieved an accuracy of 88.82% on the Spam Archive data set with color features and in [5], another method is proposed using the gradient histogram inorder to represent images. The histogram is divided into five values. The authors employed an MLP as classifier. The training is conducted using 80% of the images and the MLP achieves an accuracy of 92.7%. In [6], authors suggested SVM and PSO on 10 metadata features and 3 textual features for image spam classification. They mainly focused on SVM for recognition and Particle Swarm Optimization (PSO) to invent on maximum of the SVM results.

Deep Learning techniques can be implemented in place of ML-based approaches which necessitates manual feature engineering. In [7], the performance of several CNN based models is studied for image spam recognition. VGG, Weighted Spatial Pyramid (WSP) network and Spatial Pyramid Pooling (SPP) network-based CNN models were used there. WSP network achieved higher accuracy than other models. In [8], Instagram image spam detection, also CNN models are used. Four architectures of CNN are used i.e., three and five-level CNNs, VGG-16 and AlexNet. The results showed that the highest accuracy achieved is 84.2% by using VGG16.

1.2 Need for the study

Spam embraces counterfeit offers that could cost us time and money. One such example is Jeremy James, one of the spammers who earned $24 million by selling fake goods, services etc. via spam. Typically, spam offers some doubtful job offers, financial services, impotence treatments and invitations to some unwanted websites. Text based spam email content is somewhat similar to image spam content. It can be alleged that the used images in image spam is a screen shot of the usual text-based spam email. All targets are seen in the image with all details that spammer want to share for users i.e., if spammer wants to show ads in image spam, it may contain product name, description of the product, producer name, address, telephone number, etc. Image spam is usually a hyperlink to a website. After clicking on image, user can be able to see the special website which may contain all description of spammer target with whole details. Because of user's curiousness, by a simple click the hyper linked website gets opened. Spam messages are causing huge loss to organizations. Several resources are getting misused like mail server space, spam filtering, mail server processing. Attackers may forward bogus products sites, an authenticated site spreading fake news and providing wrong information to the users.

In recent years, image spam is increasing abundantly with tremendous growth. A major cause is that many of the email clients are filtering the spam text emails, the subject sender and email content. In the case of image spam detection, the spam is not easily notable when text is embedded into the images. Generally, email spam is detected using the spam filters which are progressed state now and can detect most of the spam with high accuracy. But when it comes to image spam detection, it is still in emerging stage and active research is going on for detecting with high accuracy. Several methods are advanced over the years to distinguish image spam. Primarily Optical Character Recognition (OCR) techniques were used for extracting textual content in image spam detection. Image spam in the arrangement of HTML was found using the OCR methods. Spammers then came up with the captcha-based techniques to obfuscating the text in the images but still readable by the humans and difficult to detect an algorithm. This problem inspired investigators to use image processing techniques for image spam identification. This paper attempts to solve one such tough problem of image spam detection and discusses the results obtained to detect image spams by leveraging the control of neural networks, deep learning, transfer learning and cost-sensitive learning. Since the beginning of deep learning, there is not much study done on this field using them.

1.3 Major contributions of the study

To fill the break in literature, in this paper, Deep Convolutional Neural Network models, transfer learning and cost-sensitive learning-based approaches are used. Hybrid model with a CNN network utilizing various ML classifiers are also employed. Comparison of cost-sensitive and cost-insensitive learning approach to handle data imbalance on various ML classifiers are also studied. Overall, the major aids of the study are:

(1) Design of two CNN models (named as CNN1 and CNN2) along with pre-trained ImageNet architecture like

VGG19 and the study of their effectiveness for image spam detection using two different datasets.

(2) Utilization of transfer learning is accomplished by using the pretrained ImageNet model such as VGG19.

(3) Comparison of cost-sensitive (by assigning class weights) and cost insensitive approach to handle imbalance of data on various ML classifiers are studied in a proposed CNN model.

(4) Finally, to find the system for detecting image spam with high accuracy and low false positive rate.

The rest of the paper is organized as follows. Section 2 presents the methodology. Section 3 contains implementation. Section 4 presents the results. Finally, the conclusion is placed in Section 5.

2. METHODOLOGY

A deep learning-based convolutional neural network method is used for image spam detection. Image spam detection is a binary classification problem and two classes are spam and ham. CNN's is used for the image processing applications since it can process the spatial information effectively by capturing the pixel-related information using the convolution on to the image with strides. The main strength of using deep learning architectures is the ability to recognize the meaning of data when it is in huge volumes and to automatically tune the resulting meaning with new data without the need for a domain expert information. The deep learning approach can give better accuracy when compared with the machine learning and also avoids the manual feature extraction task by automatically recognizing the features by itself thus reducing the time and effort. The following figure shows the generalized block diagram used for spam detection.

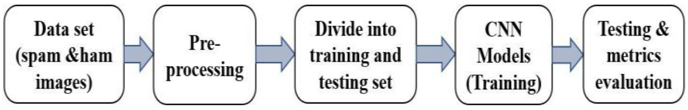

Data set (spam &ham images)
Pre-processing
Divide into training and testing set
CNN Models (Training)
Testing & metrics evaluation

Fig 2: Proposed framework for image spam identification

(A) DESCRIPTION OF DATASET

The three datasets that are used in this work are:

- Image Spam Hunter Dataset

This dataset comprises of both spam and natural images in JPEG format which are composed from original emails. 929 spam and 810 ham images from ISH dataset is used for this work.

- Improved Dataset

Improved dataset is actually a challenge dataset created in order to test the effectiveness of image spam models with more innovative spam images. It contains a total of 6,029 spam images that are generated by inserting spam text in ham images.

- Combined Dataset

In general, CNN requires large number of datasets to congregate and perform better, so instead of experimenting with individual datasets mentioned above, datasets are combined together to augment the number of spam samples. Inorder to account for the ham images, various images are downloaded. Hence, 9635 spam and 9420 ham images are employed in this work.

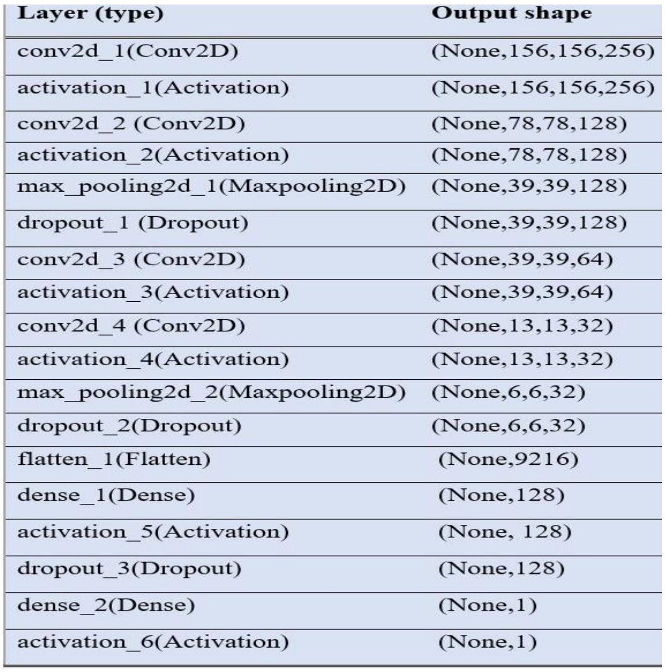
(B) PRE-PROCESSING

Datasets that are employed in this work may have a lot of identical images and corrupt files. Primarily, the corrupt files are omitted and then in order to avoid the identical files, each image is transformed into a hash and stored. So, when an identical image is read, its hash will be matched with prevailing ones. If the match is found, then the image will be neglected. Finally, all unique images are normalized and resized. The datasets used in this work is divided into 70:30 for training and testing sets.

(C) DEEP CNN MODELS

Convolutional neural network (CNN) is a highly efficient supplement to the classical feed forward network (FFN) used for classifying data predominantly image data in the field of image processing. An important aspect of deep learning is that it consists of neural network layers which automatically extracts the features from the data in hierarchical pattern and then predicts and classifies the data. Convolutional Neural Networks (CNN) idea was derived from neural networks with neurons that learns from the biases and weights. A ConvNet architecture is made from different type of layers which can be repetitive to build the deep ConvNet. In this work, for CNN1 and CNN2 models, images are resized into 156 x 156 resolution, which is opted after training and testing the model in several input sizes. CNN1 model has 2 convolutional layer of filter size 64 and 128. In CNN1, the two convolutional layers used is immediately followed by RELU activation function and max pooling layer of 3×3 area with stride 2×2 for taking maximum value. The output is flattened and given to a fully connected layer. The N vector outputs from the layer is of size 4096. On this N vector, a dense layer which contains 256 neurons is used with RELU as activation function and a dropout layer of probability with 0.1. Finally, a dense layer of single neuron which acts as output layer is added with sigmoid activation function.

CNN2 model has 4 convolutional layers of filter size 32, 64, 128 and 256. Each convolutional layer is immediately followed by the ReLU activation and maxpooling layer of pooling size 2 and 2 is employed. After the convolution layers, dropout regularization is used and the output is flattened and passed to a dense layer which contains 128 neurons. This layer is followed by ReLU activation and dropout regularization. Finally, another dense layer of size 1 which acts as the output layer is added to the end of this with sigmoid activation function. Both the CNN1 and CNN2 models are trained and tested on combined dataset for 50 epochs.



Layer (type)	Output shape
conv2d_1(Conv2D)	(None,156,156,256)
activation_1(Activation)	(None,156,156,256)
conv2d_2 (Conv2D)	(None,78,78,128)
activation_2(Activation)	(None,78,78,128)
max_pooling2d_1(Maxpooling2D)	(None,39,39,128)
dropout_1 (Dropout)	(None,39,39,128)
conv2d_3 (Conv2D)	(None,39,39,64)
activation_3(Activation)	(None,39,39,64)
conv2d_4 (Conv2D)	(None,13,13,32)
activation_4(Activation)	(None,13,13,32)
max_pooling2d_2(Maxpooling2D)	(None,6,6,32)
dropout_2(Dropout)	(None,6,6,32)
flatten_1(Flatten)	(None,9216)
dense_1(Dense)	(None,128)
activation_5(Activation)	(None, 128)
dropout_3(Dropout)	(None,128)
dense_2(Dense)	(None,1)
activation_6(Activation)	(None,1)

Fig 3: Architecture description of CNN2 model

(D) TRANSFER LEARNING

Transfer learning is also used in this work using the pretrained ImageNet model like VGG19. It refers to a technique for the analytical modeling on a different but somehow an identical problem that can then be reused partly or wholly to accelerate the training and improve the effectiveness of a model on the matter of notice. For training transfer learning based pre-trained ImageNet model like VGG19, images are resized into 256 x 256. The pre-trained last dense layer in VGG19 is omitted and to enable transfer learning all layers are frozen. Further, 3 fully connected layers of neuron 1024, 512 and 1 are added at the end and training is done with this FC layer for 50 iterations by freezing all other layers.

(E) COST-SENSITIVE & INSENSITIVE LEARNING

Cost-sensitive learning is a subfield of machine learning that takes the costs of prediction errors (and possibly other costs) into account when training a machine learning model. The main motive of this type of learning is to minimize the whole cost. In cost sensitive learning, "cost" is referred as some penalty i.e., associated with an improper prediction. Cost-sensitive learning considers dissimilar misclassifications differently compared to cost insensitive learning. That is, the cost for tagging a positive case as negative can be dissimilar from the cost for tagging a negative case as positive. Misclassification costs is not considered by the cost-insensitive model. There is a compact integrity between the imbalanced classification and cost-sensitive learning. Balanced class weights are calculated and passed to the model in cost-sensitive model while fitting process so that the model will castigate the prediction mistakes of minority class proportionally. Hybrid models are employed in this work where the features extracted from the final hidden layer of the proposed CNN3 model is passed onto many ML classifiers. ML classifiers employed in this work are Linear Support Vector Machine (LSVM), Random Forest (RF), AdaBoost (AB), K-Nearest Neighbor (KNN), Reduced Support Vector Machine (RSVM), Decision tree (DT), Linear Regression (LR) and Gaussian Naive Bayes (GNB). In this work, the comparison of cost sensitive (by incorporating weights) and cost-insensitive learning approach on the proposed CNN3 model with various ML classifiers are performed.

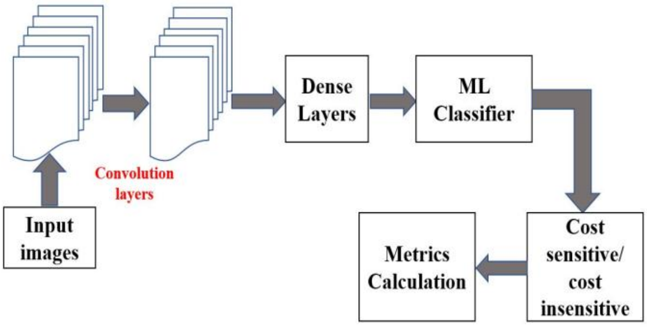


Fig 4: Overview of hybrid model

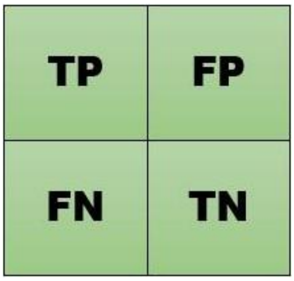
(F) TESTING AND METRICS EVALUATION

The data sets used in this work is divided into 70:30 for training and testing sets. For training, in CNN1 and CNN2 models, the images are resized into 156x156 which is fixed after training and testing the model in numerous input sizes. For training transfer learning based pre-trained ImageNet model such as VGG19, images are resized into 256 x 256. The CNN1, CNN2 and VGG models are trained and tested on the combined dataset for 50 epochs. Hybrid models are also used which extracts the features from the last hidden fully connected layer of the CNN3 and CS-CNN3 models in order to enhance the performance. CNN3 and CS- CNN3 models are trained and tested on image spam hunter dataset for 100 epochs. The binary cross-entropy loss function and Adam optimizer is used in this work.

The following metrics were used to quantify the results.

- True Positive (TP): It indicates the number of spam images that are accurately predicted as spam.
- True Negative (TN): Refers to the number of normal images that are accurately predicted as ham.
- False Positive (FP): Indicates the number of normal images that are wrongly predicted as spam.
- False Negative (FN): Refers to the number of spam images that are wrongly predicted as normal.

- Confusion matrix: It is a table used to evaluate the performance of classifier model which comprises of TP, TN, FP and FN.



TP	FP
FN	TN

Fig 5: Confusion Matrix

- Accuracy can be defined as the fraction of number of correct predictions to the total number of samples.

$$\text{Accuracy}=\frac{TP+TN}{P+N}$$

where P(Positive)=TP+FN and N(Negative)=TN+FP

- Precision is the ratio of correct positive predictions to the total predictive positives.
- Recall or sensitivity is calculated as the fraction of true positives that are properly identified.
- f1 score is the weighted mean of precision and recall.
- ROC curve is the curve obtained by plotting true positive rate (TPR) versus false positive rate (FPR) for changing threshold values.
- Zone under this ROC curve is referred to as AUC value.

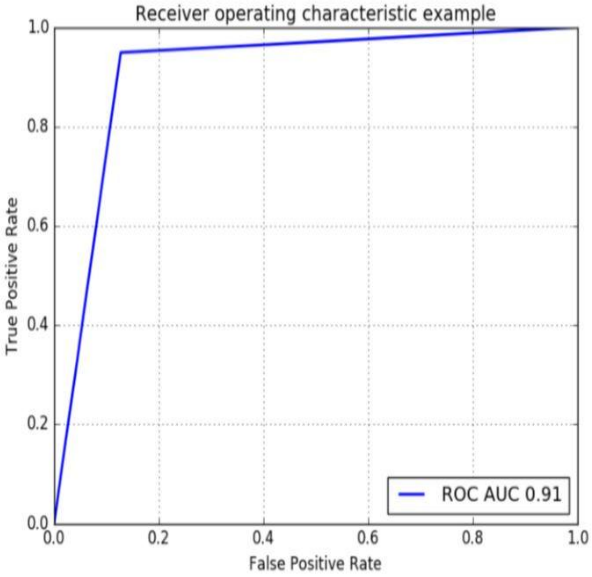


Fig 6: Example of ROC Curve

3. IMPLEMENTATION

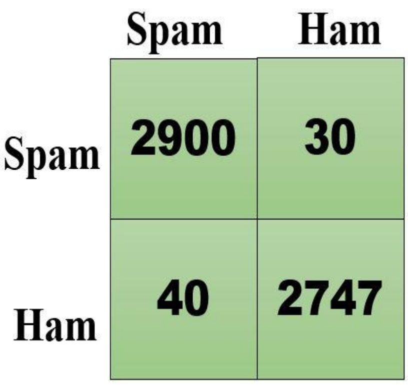
Python is the software platform used in the implementation of this project. It associates the power of general-purpose programming languages with the ease of use of domain-specific scripting languages like MATLAB or R. Keras, a deep learning framework for Python, was utilized to implement the neural network architecture for training and testing. Keras provides a layer of abstraction on top of Theano, which is used as the main neural network framework. Keras based on a Python environment, gives users the independence to use extra Python dependencies, including SciPy and PIL.

Algorithm for spam identification

```
Input: A set of images extracted from different sources $xm_1$, $xm_2$, $xm_3$, ……, $xm_n$
Output: Labels $y_1$, $y_2$, $y_3$, ……., $y_n$ (0: Ham or 1: Spam)
Pre-processing: Images are resized into essential size
1. for every extracted image $c_o$
    2. Move the take out image into the model in order to extract vector $v_i$.
    3. Calculate $c_i$ = Dense Layer($v_i$)
    4. Compute $y_i$ = Sigmoid($c_i$)
```

4. RESULTS

CNN1, CNN2 and pre-trained VGG19 model are trained for 50 iterations. For the combined dataset, CNN1 model has obtained an accuracy of 0.904 i.e., 90.4%. After testing, got 5438 correct predictions out of 5717 testing data sets. CNN2 model has obtained an accuracy of 0.932 i.e., 93.2%. CNN2 model after testing, got 5499 correct predictions out of 5717 testing samples. For pre-trained model such as VGG19, the images are resized into the resolution of 224 x 224. VGG19 model has obtained an accuracy of 0.965 i.e., 96.5%. It can be observed from table that the performance of VGG19 is better than the CNN1 and CNN2 models. VGG19 model obtained improved results than CNN2 model even if it has a smaller number of trainable parameter than CNN2 model. It may be because of the distribution of pre-trained weights as part of transfer learning.



	Spam	Ham
Spam	2900	30
Ham	40	2747

Fig 7: Confusion matrix of VGG19 model

Table -1: Performance of CNN1, CNN2 and VGG19 model

Model	Accuracy	Precision	Recall	f1-score	TP	FN	FP	TN
CNN1	0.904	0.936	0.945	0.921	2739	159	120	2699
CNN2	0.932	0.942	0.947	0.937	2819	120	98	2680
VGG19	0.965	0.970	0.952	0.943	2900	40	30	2747

Table -2: Performance of CNN3, CS-CNN3 and hybrid models

Model	Accuracy	Precision	Recall	f1-score	TP	FN	FP	TN
CNN3	0.970	0.952	0.979	0.969	260	5	10	238
CS-CNN3	0.974	0.983	0.962	0.972	266	9	4	234
CNN3-LR	0.968	0.968	0.952	0.963	261	7	9	236
CS-CNN3-LR	0.972	0.975	0.973	0.976	263	6	7	237
CNN3-RF	0.964	0.963	0.965	0.968	261	9	9	234
CS-CNN3-RF	0.986	0.982	0.981	0.985	266	8	2	237
CNN3-KNN	0.966	0.962	0.964	0.965	262	9	8	234
CS-CNN3-KNN	0.974	0.973	0.975	0.971	266	7	4	236
CNN3-DT	0.968	0.966	0.965	0.963	261	8	9	235
CS-CNN3-DT	0.965	0.967	0.965	0.966	260	6	10	237
CNN3-GNB	0.966	0.962	0.965	0.964	263	10	7	233
CS-CNN3-GNB	0.968	0.965	0.964	0.968	264	11	6	232
CNN3-AB	0.974	0.972	0.973	0.975	263	6	7	237
CS-CNN3-AB	0.978	0.975	0.973	0.976	265	5	6	237
CNN3-LSVM	0.960	0.963	0.965	0.968	261	7	9	236
CS-CNN3-LSVM	0.971	0.975	0.978	0.976	265	5	5	238
CNN3-RSVM	0.953	0.956	0.958	0.957	253	7	17	236
CS-CNN3-RSVM	0.964	0.963	0.965	0.961	265	5	5	238

Balanced class weights are calculated and passed to the CNN3 model while fitting process so that the model will castigate the prediction errors of minority class correspondingly. This approach is employed in this work and they are referred to as CS-CNN3. The CNN3 and CS-CNN3 models are trained and tested on the image spam hunter dataset for 100 epochs. Hybrid models are also used which extracts the features from the last hidden dense layer of the CNN3 and CS-CNN3 models in order to enhance the performance.

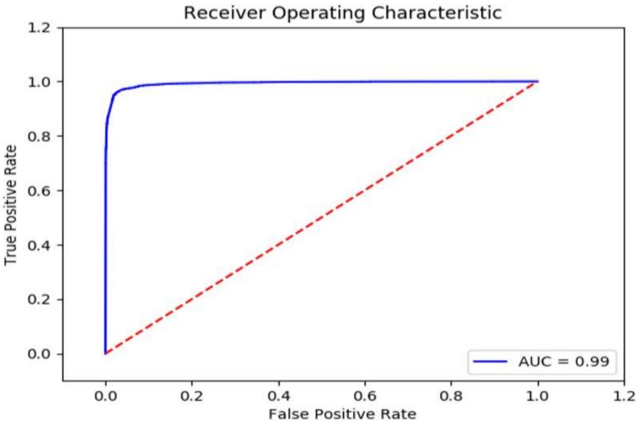


Fig 8: ROC curve of VGG19 model on combined dataset.

Cost-sensitive Random Forest classifier gives a higher accuracy of 98.6%. Various classifiers involved are LR-Logistic Regression, RF- Random Forest, KNN- K nearest Neighbor, DT- Decision Tree, GNB-Gaussian Naive Bayes, AB-AbaBoost, LSVM-Linear SVM and RSVM- Reduced SVM. With the CS-CNN3 Random Forest model, this work obtains a low false positive value of 2. Random forests are considered as highly accurate and robust method in order to enhance the performance.

5. CONCLUSION

In this research, convolutional neural network (CNN) is the deep learning network architecture used for image spam detection. Image spam detection is a binary classification problem and two classes are spam and ham. CNN is used for the image processing applications since it can process the spatial information efficiently by taking the pixel-related information using the convolution on to the image with strides. The effectiveness of three Deep Convolutional Neural Networks and hybrid models are studied for image spam detection. Comparison of cost-sensitive and in-sensitive learning are studied by assigning balanced class weights on proposed CNN3 model with various ML classifiers. Cost-sensitive Random Forest classifier gives a higher accuracy of 98.6%. Some of the proposed models performed better than existing works and some of them did not. It can be deduced that in order to form an improved image spam classifier, extra information like metadata should also be combined into the model training. In upcoming works, the properties of adversarial samples, which are capable of misleading the model to make an improper prediction, can also be studied. The object segmentation using CNN and RNN (Recurrent Neural Networks) can be used to detect the segmented region of spams and remove them from the images by deducing the background from ham images. Using such techniques, spam images can be converted into ham dynamically.

REFERENCES

[1] G Fumera, I Pillai and F Roli, “Spam Filtering based on the Analysis of Text Information Embedded into Images”, Journal of Machine Learning Research, vol. 7, pp. 2699–2720,2006.720,2006.
[2] Y.Gao, M.Yang, X.Zhao, B.Pardo, Y.Wu, T.N.Pappas, and A.Choudhary, “Image Spam Hunter”, in IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2008, pp. 1765–1768.
[3] B. Mehta, S. Nangia, M. Gupta, and W. Nejdl, “Detecting Image Spam using Visual Features and near Duplicate Detection”, in Proceedings of the International Conference on World Wide Web (WWW), 2008, pp. 497–506.
[4] M. Soranamageswari and C. Meena, “Statistical Feature Extraction for Classification of Image Spam using Artificial Neural Networks”, in Proceedings of the International Conference on Machine Learning and Computing (ICMLC),2010, pp. 101–105.
[5] M. Soranamageswari and C. Meena, “A Novel Approach Towards Image Spam Classification”, International Journal of Computer Theory and Engineering, vol.3, no. 1,2011, pp. 84–88.
[6] T Kumerasan and S Sanjushree, “Image Spam Filtering Using SVMs And Particle Swarm Optimization”,in Proceedings of the International Symposium on Computing Applications, 2015, pp. 447–490.
[7] F. Aiwan and Y. Zhaofeng, “Image Spam Filtering Using Convolutional Neural Networks,” Personal and Ubiquitous Computing, vol. 22, no. 5-6, pp. 1029–1037, 2018.
[8] C. Fatichah, W. F. Lazuardi, D. A. Navastara, N. Suciati, and A. Munif, “Image Spam Detection on Instagram Using Convolutional Neural Network,” in Intelligent and Interactive Computing. Springer, 2019, pp. 295–303.
[9] A. Chavda, K. Potika, F. Di Troia, and M. Stamp, “Support Vector Machines for Image Spam Analysis.” in ICETE (1), 2018, pp. 597–607.
[10] A. Annadatha and M. Stamp, “Image Spam Analysis and Detection,” Journal of Computer Virology and Hacking Techniques, vol. 14, no. 1, pp. 39–52, 2018.
[11] A.D. Kumar, S.KP, “Deepimagespam: Deep Learning-Based Image Spam Detection,” arXiv preprint arXiv:1810.03977, 2018.
[12] Otavia and Bruno, “Detecting Image Spam with Artificial Neural Model”, in International Journal of Computer Science and Information Security, Vol. 15,2017 No.1.
[13] A.Attar, R.M.Rad and R.E. Atani, “A Survey Of Image Spamming and Filtering Techniques”, Artificial Intelligence Review, vol. 40, pp. 71–105, 2013.
[14] M Chowdhary, J Gao, “Image Spam Classification using Neural Networks”, Review, vol. 40,2013, pp. 71–105.