Detection Of Malicious Jpeg Images Using Machine Learning

Muhammed Arshad P.P[1], Sooraj Sundaran[2], Thomas George[3], Vishnunath M.S[4], Divya K.S[5]
Dr.Vidhya P.M[6]
[1, 2, 3, 4] Dept of CSE
[5, 6]Assistant Professor, Dept of CSE
[1, 2, 3, 4, 5, 6] SNGCE, Kadayiruppu, Kerala

Abstract- *Malware is basically a software or a piece of code which remains undetected and damages the infected system. Cyber criminals are always looking for effective vectors to deliver malware to victims in order to launch an attack.Images are used on a daily basis by millions of people around the world, and most users consider images to be safe for use, however some types of images can contain a malicious payload and perform harmful ac-tions.Attackers can achieve different goals by launching an attack those goals may include stealing of important information from networks and getting remote access of the systems. With new discoveries in technology, attackers always modernize their me-thods to attack.This is where the detection of mali-cious JPEG image comes in. Captcha and by using this technique attackers can intrude into the users system.So we present a Machine Learning ap-proachby using LightGBM and Random forest clas-sifier to detect known and unknown malwares.This approach can be implemented or helpful to cloud services (e.g., Microsoft Office 365, Google Drive, etc.), social media (Facebook, Instagram, etc.), and their users from malicious JPEG images.*

Keywords- Literature survey, JPEG Images, Feature Extraction, Malware, Machine Learning, Cyber Attacks

I. INTRODUCTION

Malware is basically a software or a piece of code which remains undetected and damagesthe infected system.Cybercriminals use JPEG images to carry out their malware attacks with malware embedded in the JPEG image. There are many ways like Phishing, Baiting, Tailgating and Quid pro quo which are used by attackers to harm networks, systems and databases.While evolving the old age techniques into advanced forms, the malware activities are also updated. Attackers achieve different goals by attacking systems and networks; those goals may include stealing of important information from networks or databases and getting remote access of the systems. There are some benefits involved for which these attacking activities are led by the cyber-criminals. Advancement in technology and different means of attacks are updated in parallel. With new discoveries and innovations in technology, attackers always modernize their methods to attack. This is where the detection of malicious JPEG image comes in. This method will prevent the attack from cyber terrorists or cyber attackers. it would be valuable to implement MalJPEG, in order to protect organizations, cloud services (e.g., Microsoft Office 365, Google Drive, etc.), social media (Facebook, Instagram, etc.), and theirusers from malicious JPEG images.

II. MALICIOUS JPEG IMAGES

There’s a bit of a myth that JPEG files can’t contain viruses. This isn’t true JPEG can contain a virus. However, for the virus to be activated the JPEG files needs to be executed or run. Because a JPEG file is an image file the virus won’t be released until the image is processed.The truth is that image can play a big part in hiding malicious code,For instance a JPEG or other types of images file can easily contain additional bit of data without noticeably affecting the image’s appearance. This additional data can include code,Which is encrypted to make it harder to identify such an image can’t do much by itself.

III. COMPARISON STUDY FOR DETECTION OF MALWARE IN JPEG IMAGE

Inthis modern era thereare different methods for detecting malicious JPEG images.In this literature part of the study, definition and citations from other authors of the dependent and independent variables in the similar area of research will be presented here.

In this paper, they present MalJPEG, the first machine learning-basedsolution tailored specifically at the efficient detection of unknown malicious JPEG images[1].MalJPEG statically extracts 10 simple yet discriminative features from the JPEG file structure and leverages them with a machine learning classifier, in order to discriminate between benign and malicious JPEG images. They evaluated MalJPEG extensively on a real-world representative collection of 156,818 images which contains 155,013 (98.85%) benign and 1,805 (1.15%) malicious images. The results show that MalJPEG, when used with the LightGBM classifier, demonstrates the highest detection capabilities, with anarea under the receiver operating characteristic curve (AUC)of 0.997, true positive rate (TPR) of 0.951, and a very lowfalse positive rate (FPR) of 0.004. The problem identified in this paper was the slower execution speed due to the file leverage and the feature extraction method adapted.

People are hyper connected with each other and they arecontinuously sharing the information. For criminals, deploying malware in such scenario is very easy and propagating malware through JPEG images is one of the best and most advanced method[2]. Using steganography techniques, criminals embedded the malicious codes with legitimate or innocent looking images. These malicious content is just few line of codes which exploit the vulnerability of application. It give remote access of this system to the attacker which can do criminal act. In this framework, their primary purpose is to find the presence of any code or data in image. After it, the major section of this framework based upon the finding of code and its adverse effects. This framework show the corresponding solution to the malicious code presence in JPEG images which are spreading through online social networking sites. The drawback of this paper was this technic wont work in compressed images.

Security threats in systems and networks which are caused by malicious images, are needed to be minimized by introducing a detection technique, a technique which can involve features of headers[3]. In this proposed method JPEG headers are transformed into grayscale images to employ classification. Convolutional

Neural Network based model is proposed which aims the detection of malicious images. They have used a dataset of JPEGs which was collected from different honeypots installed by CRC of Bahria University. Dataset contains 1100 malicious and 1100 benign images to employ the detection method based on deep learning. They have achieved 86% accuracy. The main issue with this paper was lot of training data was required inorder to train with CNN.

For the detection of JPEG compression forensics [4], this paper proposes the feature vector that extracted using the Hu invariant moment of the forged image. The defined seven dimensionality feature vector is trained in an Support Vector Machine classifier for the JC detection of the forged images. The performance of the JCD is measured with several types of images: unaltered, JPEG compressed, JPEG double compressed and rotated, results of the JC classification are 0.9 over on the trained SVM classifier. Due to the usage of SVM the dataset is limited. So with this issue the efficiency was low.

The manipulated images can easily be used with malicious intentions in important fields such as law, medicine and communication[5]. In this study, an image forgery detection system is proposed by combining three deep neural network structures in parallel, unlike the uniform deep learning methods used in image forgery detection. The proposed method has been evaluated on three different dataset, due to this the working was very complex and this affected the execution speed.

Current methods for the detection of malicious codes require much improvement over the use of the same size dataset images and poor features of greyscale images[6]. This paper cites a method using the SPP-net model which can accept images of various sizes as input and also color images which provide many features for the detection of variants. Since the addition of a sublayer is required frequently, deep learning concept is incorporated. Also, they improve the detection of malicious variants too. Experimentation is done using CNN for the classification and SPP- net for various size images. Thus, the CNN architecture used in this proposed work is VGG16 which can deal with large scale recognition.

In a complicated cloud storage environment in which users upload a large number of files everyday, in order to better solve the challenge of inefficient malicious detection [7], they propose a malicious file detection method which is based on image texture analysis and BP neural network algorithm. By combining the technology of image analysis and the malicious file detection, the malicious file is converted into grayscale image, the GLCM (Ground Launched Cruise Missile) and the GIST (Generalized Search Trees) algorithms are used to extract the texture features, and the BP neural network algorithm is then used for learning and training. In thispaper,proposes and implement a malicious file detection system by means of image texture extraction. Through the experimental analysis on a large number of virus samples from the VirusShare project.

The authors[8] have proposedan image classification algorithm on improved AlexNet is proposed and designed. After preprocessing the collected images, such as normalization, mean value and standardization, the convolutional nerve is introduced to train the features of the standard images. On this basis, the image classification algorithm model based on improved AlexNet is established. Through the optimization training of the classification model, the high-level semantic features of the image are extracted, and the process of image classification and calculation is realized. The experiments show that the improved AlexNet image classification algorithm improves the accuracy and stability of image classification, and has good effectiveness in the cloud computing environment.

The authors [9] proposed in image forensics, JPEG compression history estimation problem consists of three stages: JPEG compression detection, color model identification and subsampling, and estimation of quantization steps. In this paper, a novel method for detecting JPEG compression using statistical moments of the phase spectrum is presented. The experimentation results show that the detection rates achieved by the proposed strategy are competitive with other methods reported in the state-of-the-art.

When detecting malicious code with high similarity, due to the lack of obvious training features, the detection accuracy is seriously reduced [10]. This paper proposes a malicious code detection method based on image segmentation and deep residual network. The original gray image is transformed into more distinctive sample data by image segmentation technology, which makes the data set increase the distance between classes and reduce the distance within classes, and then the feature extraction and training are carried out through the deep residual network. Malimg data set is used to test..

IV. CONCLUSION

Inthispaper,wesurveyedthelistofexistingsystems for Detection of Malicious JPEG images.We also presented astudy on JPEG Images. In the forthcoming paper, we pursue thedevelopmentof a Application for Detection of Malicious JPEG Images using Machine Learningthat will avoid all the disadvantages of the existing systems.

REFERENCES

[1] Aviad Cohen, Nir Nissim, Yuval Elovici,"MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images"– 2020

[2] Rakesh Singh Kunawar, Priyanka Sharma, “Framework to Detect Malicious Codes Embedded with JPEG Images Over Social Networking Sites” - 2019

[3] Ahsan Iqbal, Samabia Tehsin, Sumaira Kausar, Nayab Mishal, “Malicious Image Detection Using Convolutional Neural Network” –2021

[4] Kang Hyeon Rhee, “Forensic Detection of JPEG Compressed Image”– 2019

[5] Ahmet Korkmaz,CemalHanilci,“Image Forgery Detection Based on Parallel Convolutional Neural Networks” – 2022

[6] Anita Mathew, Sony Kurian, “Identification of Malicious Code Variants Using SPP-Net Model and Color Images”-2020

[7] Guanchao Wen, Yupeng HU, Chen Jiang, Na Cao, Zheng Qin , "A Image Texture and BP Neural Network BASEC Malicious Files Detection Technique For Cloud Storage Systems" – 2019

[8] Yang LU, “Image Classification Algorithm Based on Improved AlexNet in Cloud Computing Environment” – 2020

[9] Edi Morales Cruz, Jose juan Garcia Hernandez, “Detection of JPEG Compression on BitMap Image Based on Phase Spectrum Statistical features” – 2019

[10] Li Xin, Li Chao, Liang He, “Malicious Code Detection Method Based on Image Segmentation and Deep Residual Network RESNET” - 2021