

Forged File Detection and Steganographic content Identification (FFDASCI) using Deep Learning Techniques

Dr. M. Srinivas, Akshay Nayak, and Abhishek Bhatt

National Institute of Technology Warangal
Telangana, India

msv@nitw.ac.in, anayak@student.nitw.ac.in and abhishekbhatt900@gmail.com

Abstract. This paper presents our contribution in the identification and detection of Forged files and Steganographic content using Deep Neural Networks like Convolutional Neural Network and 3D-RESNET. We have used CNN in our research as CNN's are inspired by visual cortex. In other words, they are designed to extract consequential features which are relevant in classification i.e. the ones which minimize the loss function. In this the kernel weights are learned by Gradient Descent so as to generate the perceptive features from images fed to the network which in result supplemented to fully connected layer that performs the final classification task. In our proposed approach we mainly consider the two different tasks. Firstly, Identification of Forged Images has been carried out in which detection of altered images which includes both extension and signature has been performed. In addition to this, we have predicted the original epitome of forged file by using convolutional neural network model which automatically classify them and are useful for large-scale image classification as it has increased ConvNet depth. Secondly, we have recognized the Steganographic content by applying 3D-RESNET. Here, we have given preference to Residual Networks in place of VGG16 as increasing the depth should increase the accuracy of network, as long as over-fitting is taken care of. In VGG16 increased depth is increasing the effect of vanishing gradient and degradation problem. In this work, ImageCLEF 2019 data set is used for identification of Forged Images and recognized the Steganographic content.

Keywords: Transfer Learning · Optimizer · Activation Function · Loss Function · Adadelta · Categorical cross entropy · Down sampling · Memory footprint.

1 Introduction

Since the advancement of Internet, one of the important concerns has been the security of information. The creation of Cryptography has been made for securing the secrecy of communication and many methods have been identified for encrypting and decrypting data in order to keep the message secret. In addition

of keeping the contents of the message secret, it may also be necessary to keep the existence of the message secret. Here, comes the Steganography which is being considered as the art and science of invisible communication. It has been very easy to conceal confidential information inside files. Steganography [1] is the practice of concealing files, messages, images and videos within another files, messages, images or videos. The word Steganography combines the Greek words stego meaning "covered" and graphics meaning "writing". Images are one of the most usual and efficient cover media for hiding the data. There are various problems associated with file forgery which we are discussing in this paper are as follows. Firstly, the digital forensics are skipping many important and useful content during investigations. They are unknowingly treating various image files as pdf files due to the modification of those files by changing their extension to pdf format which is the major fallback in their investigation. Secondly, there is a chance of sharing of illegal information by hiding the criminal action from the plain sight and invisible those files in front of investigators. Traditional based features extraction techniques [2] are more complicated, not optimized one and lack of discriminative capacity for stego images. By using deep learning based features give high level semantic information and more discriminate [3].

This paper, reconciles the above-mentioned problems by using deep neural networks. Few years back, due to the less availability of required efficient data set, Machine Learning algorithms were very efficient with those sized data sets. The problem with it was of defining our own features that were to be learned by our model. It was Supervised Learning which made it even more complicated and complex. As the data set grows on and we have to implement on the sufficiently large amount of data set, all these models were not be able to perform well resulting in the emergence of Deep Learning field where the whole network is not fully connected type. Only the last few layers are fully connected layers as they are connected to every element of the input volume by reducing the extra number of Hyper-parameters. Deep Learning algorithms are working very well with the large data set applying supervised learning [4] where the model itself generates the weights and its feature vectors by training the fully connected layer. This is accomplished by making the kernel smaller than the input which means that we need to store fewer parameters, which both reduces the memory requirements of the model and improves its statistical efficiency. In this work, we use ImageCLEF 2019 challenging [5] data sets. In this data set contains various kind of task related to real time applications such as ImageCLEFCoral, ImageCLEFlifelog, ImageCLEFmedical and ImageCLEFsecurity. In this work, we select the ImageCLEFsecurity related task [6] for identification of Forged Images and have recognized the Steganographic content.

1.1 Previous Research Work

There are few research works that have been performed and is going on for forged file detection and identification of steganographic content.

Forged File Detection Few research works have been performed in which the simplest and the naive method of looking only at file extensions. As there are various ways in which type of a files can be detected without even opening them. This is not very useful when one should have to detect large number of files since volume of files determine the detection speed. The use of extensions in file type detection is not efficient as extensions are easily spoofed and altered. It is easy to change the extension by several mouse clicks in various operating system. It is not necessary to open a file during classifying the files based on their extensions, in similar manner it is not necessary for to mislead these classification techniques. In open source OS like Linux, extensions are not required for the extension-based file type detection. This OS is allowing optional extensions of any string regardless of file type which results in hiding these files from an inexperienced administrator.

File Type Detection using Magic Bytes is one of the most sophisticated method for file type detection. Magic Bytes are specific to binary files and rely on matching signatures which are varying in length in file headers or tails. Due to inadequate standards for the content in files, the new file type creators will include headers for uniquely identifying files of their type. For example, letters PK has been present at the beginning of every .zip file in order to identify the Zip format files as ZIP file format had been invented by PKWARE. This method is usually slower in checking the file extension as files are being opened for reading the small number of bytes for deciding the file format. If it matches the expected result then the given file is in specific format, else it is treated as suspicious. It works only on binary file types having magic bytes associated with them. This is the cons of magic bytes type detection when the person has to consider the risk associated with ignoring detection of ASCII based files.

Steganographic Content Identification Active approach is performed for determining the steganographic images. Digital Images require pre-processing such as watermarking or signatures like fingerprinting are being generated during image creation. But this is not very efficient or useful in authenticating the image when the internet is not having the large number of water marked and digital signed images. Passive approach is the most expedient forgery detection technique called as blind forgery detection. The blind name factor ascends as it uses the received image for the originality check without any modification in image at the time of creation and capture. Copy-Move Detection Technique and Slicing are another passive approach where in the CMDT a part of an image is copied and pasted in some other location within the same image and in Slicing one or more images get combined together to form a new image. But copying a part of an image or slicing an image are not useful in finding whether an image is hiding some text behind it. Some sample of stego and non stego images are show in Fig. 1

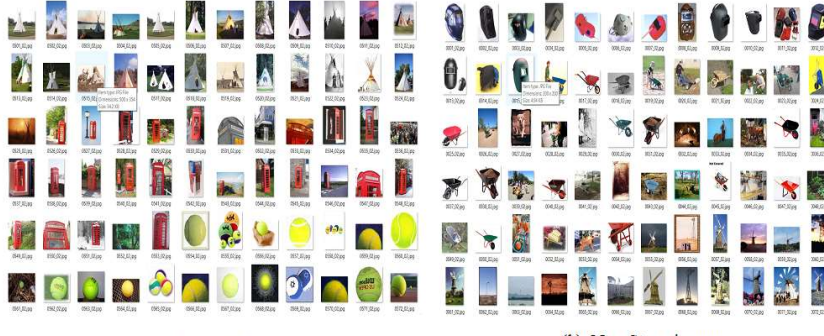


Fig. 1. Some of the stego and non-stego images samples.

1.2 Proposed Approach

For detecting a forged file, a pdf file has been given as an input to the network for reading each and every byte [7] and the frequency of each byte is being counted. After that a histogram has been plotted using the frequency distribution data table [8]. In the second stage of our work, the resulting histogram is being supplemented to VGG16 [16] which have been trained on the custom data for classifying the file types. The resulting output of the model has been predicted the actual type of file supplemented to it. The files have been predicted as images and are being stored as dataset for the next stage of proposed model resulting in classifying the image as stego or non-stego after boosting the ResNet50 [13] with image classified files.

Generally, ASCII values are varying in the range of $[0, 255]$ resulting in the availability of 256 numbers of bins in range $[0, 255]$. The x-axis represents byte value and the y-axis represents the frequency of each byte value. The histogram could be generated in two formats. 1. Grey scale format [9] and 2. RGB format [9]. We have decided to go with RGB formatted histogram as it is convenient to amplify RGB image in VGG16 network as it takes the input images in three channels. Else, we have to convert the grey scaled images to an image having 3 channels containing the same pixels for each channel. The resulting histogram has been used in the proposed model for the file type identification can be analyzed by seeing the Fig 2, in which each file type has their own histogram representation.

The histogram of each with varying file type, either may be of JPG, GIF, PNG or PDF format is different from each other. For classifying the actual file type, VGG16 [10] model plays an important role as an image classifier. We have re-trained the above mentioned VGG16 model with obtained histogram images for GIFs, JPGs, PDFs and PNGs using Transfer Learning which enables us to use pre-trained model by changing the output classifying layer. The neural network is generating "weights" by training it on very large dataset. These extracted

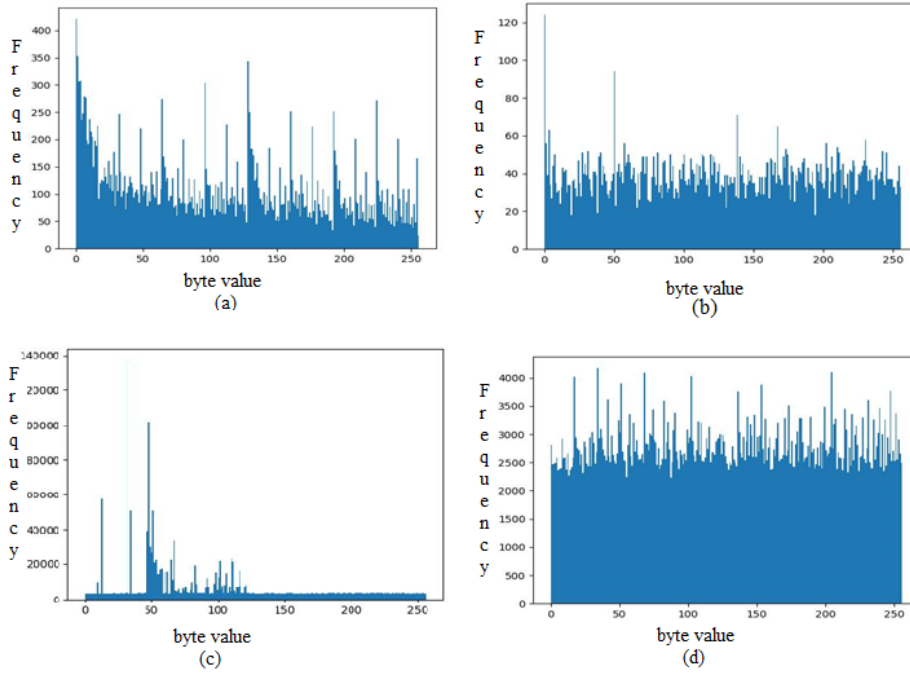


Fig. 2. Different type of files corresponding Histogram images. (a) gif file (b) jpg file (c)pdf file (d) png file related histogram images

weights then transferred to any other network which protect us from training the full network from scratch by transferring the conversant features. VGG16 is a deep convolutional neural network having different convolutional and pooling layers. After series of passage through convolutional and max pooling layer, the immediate output then supplemented to the next two fully connected layer having 4096 classes and the appearing output finally be augmented to the dense fully connected layer of four classes having SoftMax as an activation function. There are some layers present in between the convolutional and pooling layer which is called as ReLU playing an important role by only keeping the positive values. The Dense layer which is being worked as fully connected layer has SoftMax as an activation function [11] having 4 classes at last. For file forgery detection histogram based features and the fine-tuned VGG16 model is in our approach method and have shown in Fig. 3 stage-I.

After the classification of files as images using CNN based classification method, next we have crammed another network called ResNet50 [13] for to check the images are stego or non stego. We are supplementing our network with large dataset and for deep analysis we have considered ResNet50 as an important model having 50 layers for identifying the altered images hiding the steganographic content. ResNet50 has 25,583,592 trainable parameters and hav-

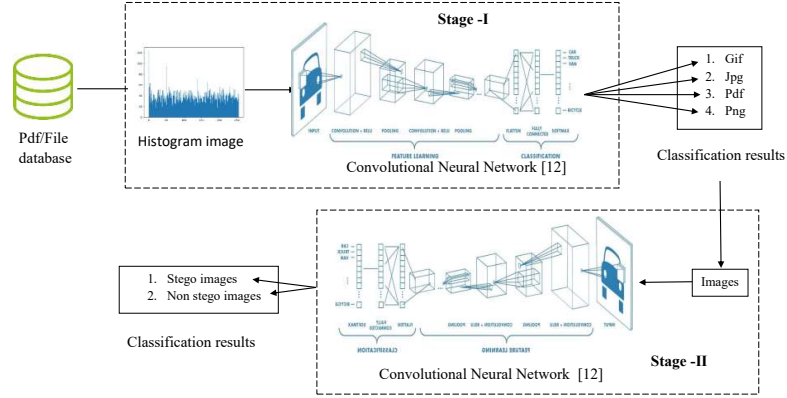


Fig. 3. Block diagram of FFDASCI model

ing 53,120 non-trainable parameters. We have trained the model with our custom dataset consisting of two types of image, one is stego images and the another is non-stego images. This time the network has been trained by the images itself instead of supplementing with the histograms of each type of images classifying the images into stego and non-stego. Fig. 3 is showing the complete architecture of the proposed model.

1.3 Dataset

In this work, we used the dataset provided by ImageCLEFsecurity 2019 [6] containing of 9,000 images for three different kind of tasks. We have supplemented our Network model with a total of 2400 histogram images of first task. We have processed the images and have used RGB format in our model. We have trained the network with the customized dataset. The root folder named data contains four sub folders named GIF, JPG, PDF and PNG containing 400, 400, 1200 and 400 histogram images respectively which are representing each of the file type. We have divided the dataset in training and testing sets and 80% of the total data from dataset is used for training our model and the remaining 20% have been used for testing purpose. In second task, dataset for stego image classification consists of 1000 images dividing into 500 stego and 500 non-stego images indexed from 0001_02 to 1000_02.

1.4 Experimental Results

In this work, the performance of the proposed system is evaluated by measuring classification accuracy. In our FFDASCI model we have considered “categorical crossentropy” [14] as the loss function, “adadelta” as an optimiser, “metrices” as

an accuracy standard and “SoftMax” as an activation function. For forgery detection task we have trained the VGG16 network on our custom forgery detection dataset for 12 epochs with 32 as batch size. We have achieved 99.93% validation accuracy and have also tested with Support Vector Machine (SVM) classifier on same forgery detection task dataset. With SVM classifier we achieved 99.73% of validation accuracy and the accuracy results are shown in Table 1.4.

Table I: Performance comparison of the proposed method with SVM classifier on forgery detection validation dataset.

Method	Accuracy (%)
Proposed Method (VGG16)	99.93
SVM	99.73

By using SVM classifier we calculate the class wise classification performance. Table 1.4 shows the class wise accuracy for the file forgery detection using SVM classifier with histogram features.

Table II: Class wise performance results of the SVM classifier on forgery detection validation dataset.

Classes	Precision	Recall	F1-score	Support
gif	1.00	1.00	1.00	69
jpg	0.99	1.00	0.99	83
pdf	1.00	1.00	1.00	138
png	1.00	0.99	0.99	79

For stego image classification task, we have trained the ResNet50 network for the same number of epochs and having batch size as similar of VGG16. We have achieved 99.9% validation accuracy with the proposed method. In this task, we have also used SVM classifier to classify the stego image and 93.5% classification results are being achieved. Table 1.4 shows the classification results of proposed method and SVM classification results On stego image data.

Table III: Performance comparison of the proposed method with SVM classifier on stego image validation dataset.

Method	Accuracy (%)
Proposed Method (ResNet50)	99.9
SVM	93.5

Table 1.4 shows the class wise accuracy for stego image discovery. We have been secured the testing accuracy of 99.90% accuracy from our proposed model.

Table IV: Class wise performance results of the SVM classifier on stego image validation dataset.

Classes	Precision	Recall	F1-score	Support
Non-Stego image	0.51	0.70	0.59	93
Stego image	0.62	0.42	0.50	107

1.5 Conclusion

The histograms produced by frequency distribution of bytes of each file type are being separate from each other for File Type Detection. We have proposed a model which is useful in classifying the forged files and have been able to classify whether the files are stego or not. We have decreased the computational time complexity in detecting the forged files and steganographic content. There is no need of opening the file for file type detection which relieves from magic bytes strategy. As if human cortex can detect the forged file images, certainly network which would be specifically designed for this is more powerful and speeding up the detection time. Our model is efficient in identifying the steganographic content which were earlier skipped by the digital investigators. Using this each and every hidden and forged files are bring able to identify and helps in investigation.

References

1. Altaay, Alaa A. Jabbar et al. An Introduction to Image Steganography Techniques. 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT) (2012): 122-126.
2. Srinivas, M., and C. Krishna Mohan. "Classification of medical images using edge-based features and sparse representation." 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2016.
3. Srinivas, Mettu, Yen-Yu Lin, and Hong-Yuan Mark Liao. "Deep dictionary learning for fine-grained image classification." 2017 IEEE International Conference on Image Processing (ICIP). IEEE, 2017.
4. Srinivas, M., Yen-Yu Lin, and Hong-Yuan Mark Liao. "Learning deep and sparse feature representation for fine-grained object recognition." 2017 IEEE International Conference on Multimedia and Expo (ICME). IEEE, 2017.
5. Bogdan Ionescu and Henning Muller and Renaud Peteri and Yashin Dicente Cid and Vitali Liauchuk and Vassili Kovalev and Dzmitri Klimuk and Aleh Tarasau and Asma Ben Abacha and Sadid A. Hasan and Vivek Datla and Joey Liu and Dina Demner-Fushman and Duc-Tien Dang-Nguyen and Luca Piras and Michael Riegler and Minh-Triet Tran and Mathias Lux and Cathal Gurrin and Obioma Pelka and Christoph M.Friedrich and Alba Garcia Seco de Herrera and Narciso Garcia and Ergina Kavallier-atou and Carlos Roberto del Blanco and Carlos Cuevas Rodriguez and Nikos Vasil-lopoulos and Konstantinos Karampidis and Jon Chamberlain and Adrian Clark and An-tonio Campello, ImageCLEF 2019: Multimedia Retrieval in Medicine, Lifelogging, Se-curity and Nature, Experimental IR Meets Multilinguality, Multimodality, and Interac-tion., Proceedings of the 10th International Conference of the CLEF Association (CLEF 2019), LNCS Lecture Notes in Computer Science, Springer, September 9-12, Lugano, Switzerland.

6. Konstantinos Karampidis, Nikos Vasillopoulos, Carlos Cuevas Rodriguez, Carlos Roberto del Blanco, Ergina Kavallieratou and Narciso Garcia. Overview of the ImageCLEFsecurity 2019 Task., CLEF working notes, CEUR, 2019.
7. Karampidis, Konstantinos, Ergina Kavallieratou, and Giorgos Papadourakis. "Comparison of Classification Algorithms for File Type Detection A Digital Forensics Perspective." POLIBITS, vol.56, 2017,pp.1520.
8. Aedla, Raju and G. S. Dwarkish and Reddy Venkat. (2013). A Comparative Analysis of Histogram Equalization based Techniques for Contrast Enhancement and Brightness Preserving. International Journal of Signal Processing, Image Processing and Pattern Recognition. vol. 6. 2013, pp. 353-366.
9. Tarun Kumar, Karun Verma, A Theory Based on Conversion of RGB image to Gray image. International Journal of Computer Application, 7(2), pp. 7-10.
10. Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." arXiv preprint arXiv:1409.1556 (2014).
11. Nwankpa, Chigozie, et al. "Activation Functions: Comparison of trends in Practice and Research for Deep Learning." arXiv preprint arXiv:1811.03378 (2018).
12. [https://www.mathworks.com/videos/introduction to deep learning what are convolutional neural networks 1489512765771.html](https://www.mathworks.com/videos/introduction%20to%20deep%20learning%20what%20are%20convolutional%20neural%20networks%201489512765771.html)
13. He, Kaiming et al. Deep Residual Learning for Image Recognition. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016): 770-778.
14. Dufourq, Emmanuel, and Bruce A. Bassett. "Automated problem identification: Re-gression vs classification via evolutionary deep networks." Proceedings of the South African Institute of Computer Scientists and Information Technologists. ACM, 2017.
15. Hara, Kensho et al. Learning Spatio-Temporal Features with 3D Residual Networks for Action Recognition. 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (2017): 3154-3160.
16. Shelhamer, Evan et al. Fully Convolutional Networks for Semantic Segmentation. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2015): 3431-3440.