A DEEP-LEARNING APPROACH FOR DETECTING SPLICING & COPY-MOVE IMAGE FORGERIES AND IMAGE RECOVERY

A PROJECT REPORT

Submitted by

Aravind J 2019115017

Krishnan S 2019115047

Pranay Varma 2019115067

submitted to the Faculty of

INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY

COLLEGE OF ENGINEERING, GUINDY

ANNA UNIVERSITY

CHENNAI 600 025

ANNA UNIVERSITY

CHENNAI - 600 025

BONA FIDE CERTIFICATE

Certified that this project report titled A DEEP-LEARNING APPROACH FOR DETECTING SPLICING & COPY-MOVE IMAGE FORGERIES AND IMAGE RECOVERY is the bona fide work of ARAVIND J, KRISHNAN S and PRANAY VARMA who carried out project work under my supervision. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion on this or any other candidate.

PLACE: Chennai
DATE: 7.12.2022

DR. K. INDRA GANDHI
Assistant Professor
PROJECT GUIDE
DEPARTMENT OF IST, CEG
ANNA UNIVERSITY
CHENNAI 600025

COUNTERSIGNED

DR.S.SRIDHAR
HEAD OF THE DEPARTMENT
DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600025

ABSTRACT

Digital picture usage has increased at a never-before-seen rate in our day and age, due to the proliferation of gadgets like smartphones and tablets. Furthermore, the development of user-friendly image manipulation software that is available at reasonable prices has made manipulating such content more effortless than ever. Some of these images are tampered with so that it is impossible for the human eye to detect. Moreover, social media platforms such as Facebook, Instagram, and Twitter have made the distribution of those images to the general public a simple task. Some of these tampered images can cause serious business or political issues. Thus it becomes very important to develop automated methods that can detect such forgeries.

Three of the most common image manipulation techniques are:

- **SPLICING**: In splicing a region from an authentic image is copied into a different image.
- **IMAGE INPAINTING**: In image inpainting, an image region is removed and the removed part is then filled in to complete the image.
- **COPY-MOVE**: A specific region from the image is copy pasted within the same image

In this research, we detect and localize splicing and copy-move image forgeries in images by using three different deep-learning techniques - Convolutional Neural Networks, Unsupervised Self-Consistency Learning and Unsupervised Domain Adaptation and attempt to recover the original image using an image tamper resilient generative scheme for image self-recovery.

ACKNOWLEDGEMENT

We would like to convey our gratitude to DR.S.SRIDHAR, Head of the Department, Department of Information Technology, College of Engineering, Guindy, Anna University, Chennai for providing us the opportunity and infrastructure to carry out this project.

We express our sincere gratitude to our guide DR.K.INDRA GANDHI, Assistant Professor,Department of Information Technology,College of Engineering, Guindy, Anna University, Chennai for her invaluable support, guidance and encouragement for the successful completion of this project. Her knowledge, attitude, commitment and spirit have inspired and enlightened us.

We express our thanks to the panel pf reviewers DR.K.VANI, DR.S.BAMA, DR.P.GEETHA, DR.M.DEIVAMANI and DR.D.NARASHIMAN for their valuable suggestions.

And last,but not the least,we wish to thank our parents and family members for bearing with us throughout the project period and for having given us the opportunity to do this course in such a prestigious institution.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Malicious image manipulation, previously restricted to dictators and spy agencies, is now available to legions of common Internet trolls and Facebook conmen. It is now possible to create realistic image composites, fill in large image regions, generate plausible video from speech, and so on with only basic editing skills. One might have expected that these new methods for creating synthetic visual content would be accompanied by equally powerful techniques for detecting fakes, but this has not been the case thus far. Thus detecting such forgeries becomes very important to stop the spread of false information. In this research, we suggest both supervised and unsupervised methods to detect and localize image tampering.

1.2 OBJECTIVE

This research work aims to:

- Detect and localize splicing and copy-move image tamperings.
- Approximately recover the original image that was tampered with.
- Analyse the performance of different deep-learning approaches on varied test-sample difficulty.
- Develop a web application using Flask/Streamlit that will be hosted in cloud, where the users can upload the tampered images.

1.3 PROBLEM STATEMENT

The goal of this study is to detect and localize Splicing and Copy-Move forgeries in images using both supervised and unsupervised deep learning techniques. To achieve this 3 deep-learning approaches - Convolutional Neural Networks (CNN), unsupervised self-consistency learning and unsupervised domain adaptation have been implemented on various image forensics datasets like CASIA2, NC16, In-the-Wild Image Splice Dataset and COCO dataset and the performance of image forgery detection for each approach is analysed based on the test sample difficulty.

This research work also aims to approximately recover the original image which is subject to splicing or copy-move tampering using an image tamper resilient generative scheme for image self-recovery.

1.4 SOLUTION OVERVIEW

CNN Approach: Various computer vision and deep-learning approaches have been suggested to detect image forgeries to date. Specifically, a few CNN-based architectures have managed to predict images with an accuracy of close to 98%. However, the tampering done in these images can be easily recognized by humans as well. In this project, we are developing a CNN network that attempts to detect forgeries on more difficult samples and analyse its performance on such examples. This is a supervised approach.

Unsupervised Self-Consistency Learning: Standard supervised learning approaches, which have been extremely successful for many types of detection problems, are unsuitable for image forensics. This is due to the vast and diverse space of manipulated images, making it unlikely that we will ever have enough manipulated training data for a supervised method to fully succeed.

To overcome this, we are using an unsupervised methodology called self-consistency learning where with the help of EXIF metadata, we can identify if the image has been tampered with. EXIF tags are camera specifications that are digitally engraved into an image file at the time of capture. Thus, given two photographs, we can figure out from their EXIF metadata that there are a number of differences in the two imaging pipelines.

1.5 ORGANIZATION OF THE REPORT

The organization of report is as follows.Chapter 1 gives a background information,objective and the problem statement. Chapter 2 gives the literature survey,the methods that can be implemented for detecting tampered images and the image reconstruction.Chapter 3 elaborates on the technical architecture,function of each module and the working of each ,module.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

The detection of a forged image is driven by the need for authenticity and to maintain the integrity of the image. There are cases when it is difficult to identify the edited region from the original image. Various computer vision and deep-learning approaches have been suggested to detect image forgeries to date. While some of these approaches had very high accuracy, they were tested on less challenging datasets. A literature survey was done to gain better insights into the existing solutions and their performance on different test samples. The limitations and the knowledge gained from the papers will help us to create a better system.

2.2 SUPERVISED LEARNING APPROACHES

2.2.1 AN EFFICIENT CNN MODEL TO DETECT COPY-MOVE IMAGE FORGERY [1]

This paper introduced an accurate deep CMF detection method. The traditional approach uses a block-based algorithm, whereas the CNN approach uses the entire image. The proposed method is divided into three stages: preprocessing, feature extraction, and classification. The input image is resized to enter the next stage without cropping any image parts in the preprocessing data stage. Three convolution layers are followed by a max-pooling layer in the feature extraction stage. At the end of this stage, a full connection layer connects

all features to the dense layer. Finally, the classification stage is invoked to categorise the data into two groups (forged or original).

With an appropriate number of convolutional and max-pooling layers, the proposed architecture is computationally lightweight. The approach also offers a quick and accurate testing process that takes 0.83 seconds for each test. Many empirical experiments have been carried out to ensure the proposed model's efficiency in terms of accuracy and time. These tests were carried out on benchmark datasets and achieved very high accuracy.

However, the accuracy of classification in this approach is not so good when the test samples are challenging.

2.2.2 COPY MOVE AND SPLICING IMAGE FORGERY DETECTION USING CNN [2]

This paper presents an approach to detecting copy move and splicing image forgery using a Convolutional Neural Network (CNN) with three different models i.e. ELA (Error Level Analysis), VGG16 and VGG19. Two datasets of varying difficulty, CASIA v2.0 and NC2016 are used.

The major components of the proposed methodology are, pre-processing, error level analysis and CNN.

In the preprocessing stage, the dataset is resized to 128*128 pixels. The ELA stage involves resaving the preprocessed images, resulting in an increase in brightness. The resaved images are compared to the preprocessed ones, with forged images having a greater brightness in their modified components with respect to the original portions. Next, the image is resized with each RGB value normalized between 0 to 1. Finally, CNN-based training

occurs with two architectures (VGG16 and VGG19) being utilized.

The experimental results validate that the classification performance decreases when the samples are more challenging. The implemented architecture does not easily generalize to datasets with different underlying distributions.

2.2.3 A DEEP LEARNING APPROACH TO DETECTION OF SPLICING AND COPY-MOVE FORGERIES IN IMAGES [3]

In this paper, a new deep learning-based image forgery detection method that uses a convolutional neural network (CNN) to automatically learn hierarchical representations from input RGB colour images has been presented. The proposed CNN is intended primarily for image splicing and copy-move detection applications. Rather than using a random strategy, the weights in the network's first layer are initialised with the basic high-pass filter set used in the calculation of residual maps in the spatial rich model (SRM), which serves as a regularizer to efficiently suppress the effect of image contents and capture the subtle artifacts introduced by tampering operations. To extract dense features from the test images, the pre-trained CNN is used as a patch descriptor, and a feature fusion technique is used.

The proposed solution outperforms many state-of-the-art models, in terms of speed and accuracy, however, the performance of the model deteriorates for more challenging image forgery datasets.

2.3 UNSUPERVISED LEARNING APPROACHES

2.3.1 FIGHTING FAKE NEWS: IMAGE SPLICE DETECTION VIA LEARNED SELF-CONSISTENCY [4]

In this paper, a learning algorithm has been proposed for detecting visual image manipulations that have been trained solely on a large dataset of real photographs. The algorithm employs the automatically recorded photo EXIF metadata as a supervisory signal for training a model to determine whether an image is self-consistent, or whether its content could have been produced by a single imaging pipeline. This self-consistency model is applied to the task of detecting and localising image splices. The insight explored in this paper is that patches from a spliced image are typically produced by different imaging pipelines, as indicated by the EXIF meta-data of the two source images.

Despite never seeing any manipulated images during training, the proposed method achieves state-of-the-art performance on several image forensics benchmarks.

However, the model is not well-suited to finding very small splices in images. Also, over and underexposed regions are sometimes flagged by the model to be inconsistent because they lack any meta-data signal.

2.3.2 FORGERY CLASSIFICATION VIA UNSUPERVISED DOMAIN ADAPTATION [5]

In this paper, two major steps are involved in the detection of copy-move forgeries in images: Dataset Generation and Forgery Classification using Domain Adaptation. Two methods are employed to generate the dataset.

Semantic Inpainting helps the model to learn edge discrepancies when the objects are removed, while Copy-Move tampered images improve the focus of the network to recognize similar patches.

The COCO dataset acts as the base for generating tampered images. The generated dataset contains 80,000 images of which 60,000 are generated through copy-move forgery and 20,000 through semantic inpainting.

For domain adaptation, the authors have applied two methods; Domain Adversarial Neural Network (DANN) and Deep Domain Confusion (DDC). Both approaches have a discriminative base model, and the weights between the layers are shared. The adversarial loss in the case of DANN is minimax, whereas, in DDC, it's confusion loss. The Casia and CoMoFoD datasets acted as target domains, with tests performed on Casia producing more accurate classifications when compared to those performed on CoMoFoD.

2.4 IMAGE RECONSTRUCTION

2.4.1 FROM IMAGE TO IMUGE: IMMUNIZED IMAGE GENERATION [6]

The authors propose a system to produce tamper-resilient images. The steps involved in the approach involve training a U-Net backboned encoder, a tamper localization network and a decoder for image recovery. The objective is to convert normal images into immunized images and to conduct successful tamper localization and content recovery on them at the recipient's side. Imuge is designed to be robust against common attacks such as lossy compression, image interpolation or cropping. One of the concerns of the authors is for the differences between the encoded or 'immunized' images and the original images to be imperceptible.

The encoded images are subjected to 5 types of attacks and 2 kinds of malicious tampering. The tampered image is then passed through a verifying layer, which predicts the tamper mask of the attacked image and generates the rectified image. Finally, the decoder generates the recovered image given the rectified image. The system performs well in detecting different kinds of tampering and reconstruction is satisfactory, both in terms of the quality of the image and accuracy with respect to the original version.

2.5 SUMMARY

Hence there are many methodologies we studied from the research papers.For the first phase of our project we will be implementing the image forgery detection by CNN and Unsupervised self consistency.In the second phase we will be reconstructing the tampered image to original image.

CHAPTER 3

SYSTEM DESIGN

3.1 INTRODUCTION

The approaches that have been implemented to detect copy-move and splicing tampering in images are CNN, a supervised learning approach and Self-Consistency Learning, an unsupervised learning method. Two different datasets of varying difficulty have been used to test both these approaches. The first dataset used is the 'CASIA 2 Image Forensics' dataset, which has 12,622 images, where the ratio of authentic to tampered images is 60:40. The tampering in this dataset is less challenging and can be recognized by humans.

The second dataset used is the 'Labels in the Wild' dataset which contains 201 tampered images and the masks of each tampered image. This dataset is relatively much more challenging than the CASIA 2 dataset and the tampering cannot be easily recognized by humans. Both approaches' classification accuracy is evaluated using these two datasets.

3.2 TECHNICAL ARCHITECTURE

3.2.1 CNN APPROACH

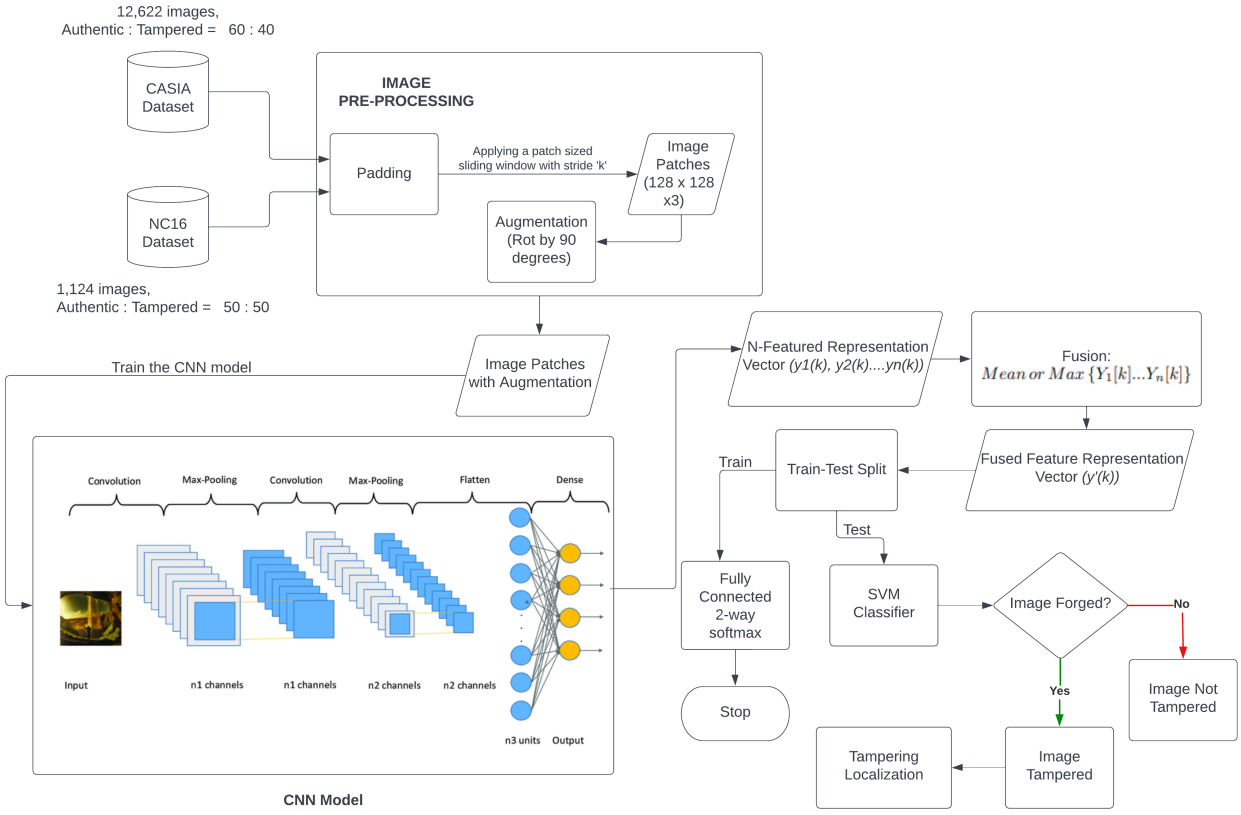


Figure 3.2.1: CNN Approach Architecture

3.2.2 UNSUPERVISED SELF-CONSISTENCY LEARNING

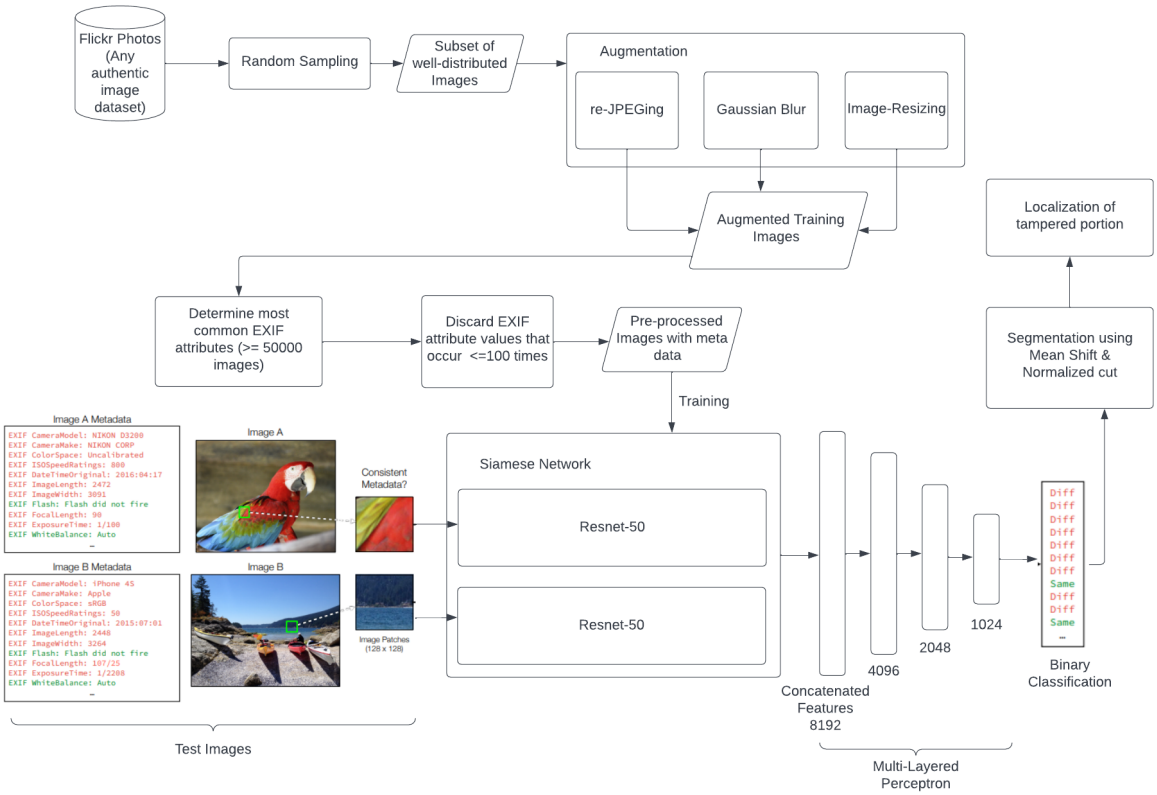


Figure 3.2.2: Self-Consistency Learning Architecture

3.3 CNN MODULES

3.3.1 PATCH EXTRACTOR

For each image in the authentic and tampered class in the dataset, a patch having a window size 128 x 128 x 3 (Width x Height x Number of Channels) is applied and the window is slid based on the stride value. Here, we are using a stride of 128 and 2 patches are extracted per image so that training of the CNN model becomes less computationally expensive.

To identify the exact patch which is tampered with in the images of the tampered class, the masks of the image are analysed and the region where the number of zeros (the black portion in the image mask) is less than or equal to 99% of the total number of zeros and ones combined is flagged as a tampered patch.

Then the extracted patches are augmented by rotating them by 0, 90, 180 and 270 degrees, thereby resulting in 8 patches per image. The module programmatically creates directories for storing the extracted patches of the tampered and the authentic class.

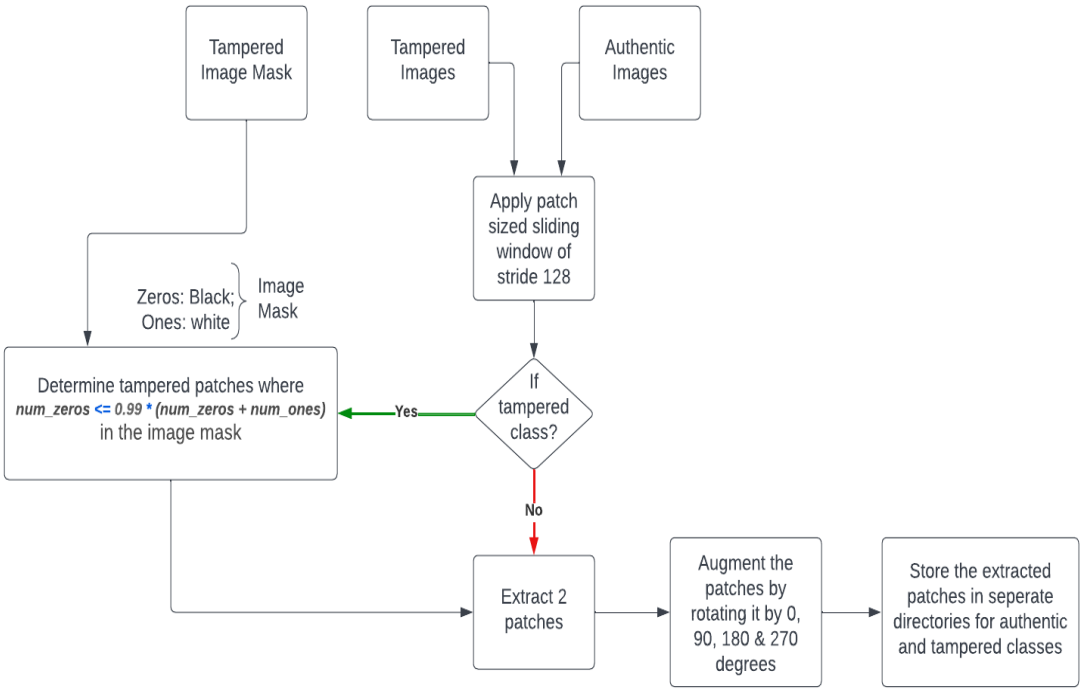


Figure 3.3.1: Patch Extraction

3.3.2 CNN MODEL AND TRAINING

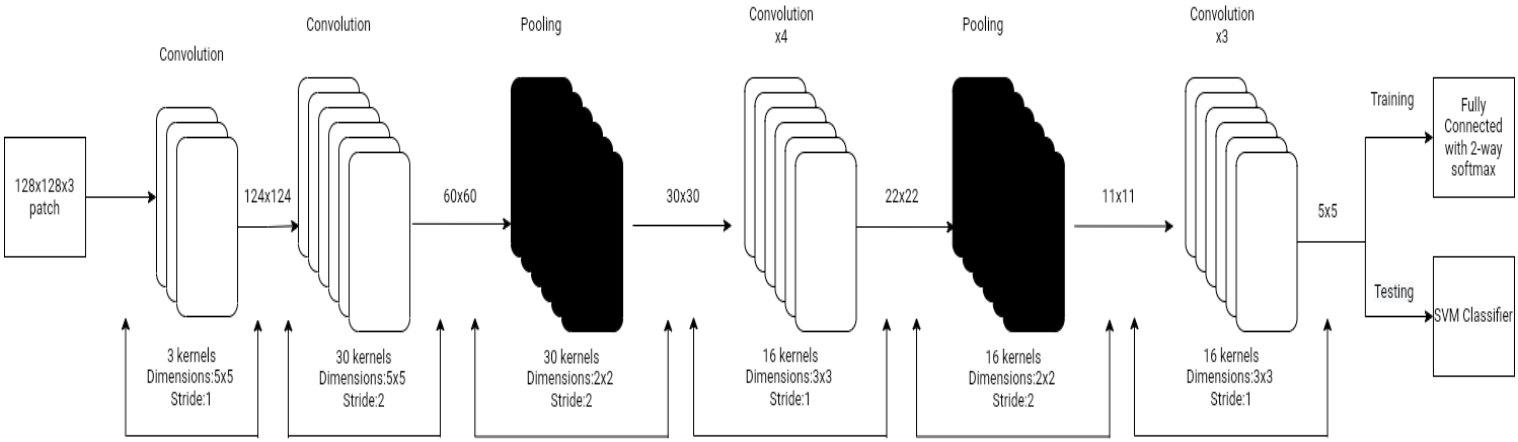


Figure 3.3.2: CNN Model and Training

The model consists of 9 convolution and 2 pooling layers. 128 x 128 x 3 patches are passed through the network for the purpose of feature extraction, with the resultant feature vector serving as an input for the SVM classifier. The first convolution layer consists of 3 5x5 kernels with a stride of 1, while the first pooling layer has 30 2x2 filters of stride 2. The second convolution layer has 30 5x5 kernels of stride 2. The next 7 convolution layers all have 16 3x3 filters of stride 1, while the other pooling layer has 16 2x2 filters of stride 2.

The convolution layers extract features from the input matrices, while the pooling layers perform down-sampling or dimensionality reduction of the features. The ReLu activation function is used by each of the convolution layers. Local response normalization is applied to every feature map before the pooling operation to improve generalization. As far as training is concerned, two random tampered patches are selected per image as training a huge amount of extracted patches would be computationally expensive. The model is trained for 250 epochs

3.3.3 FEATURE EXTRACTOR AND SVM CLASSIFIER

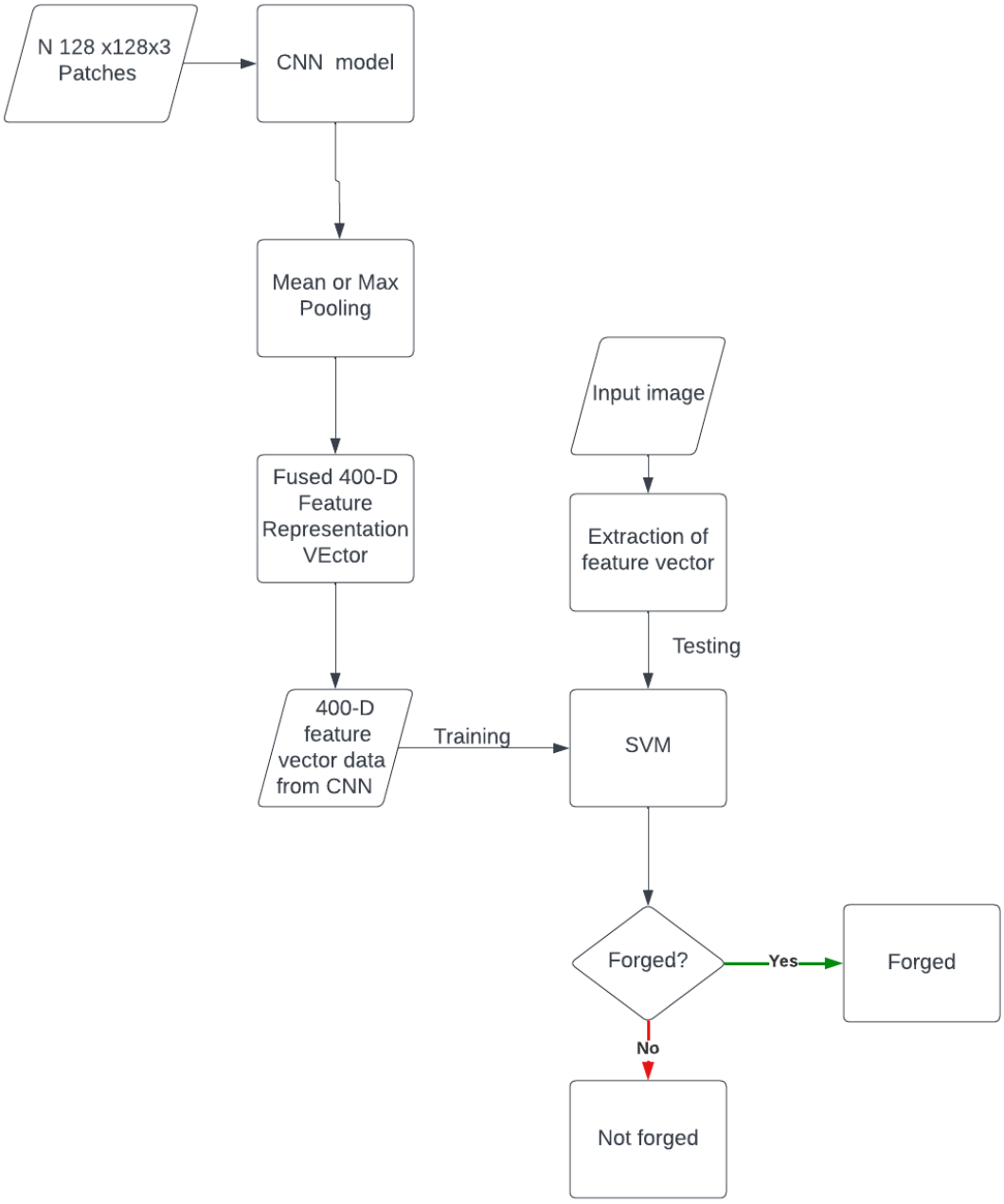


Figure 3.3.3: Feature extraction and SVM classifier

The 128x128x3 patches are fed into the CNN model, which extracts a 400-D (5x5x16) feature representation of the patches. These features are then passed to a fully-connected layer with a 2-way softmax classifier in the training phase and the SVM model in the testing phase.

Before being fed into the SVM classifier, the (n x 400-D) feature representations for an image must be fused into a single feature vector. Mean or max pooling is applied on each dimension of the representation over all the n patches to obtain the resultant fused feature vector for an image, which has 400 features.

This 400-D feature vector is used to train the SVM classifier. After training the SVM classifier, an input image can be given to the SVM model to predict whether the image has been tampered with or not.

3.3.4 TAMPER REGION LOCALIZATION

A testing image is used as the input, and a pre-trained ”ManTraNet” model is used to predict a pixel-level forgery likelihood map as the output. It is made up of two smaller networks:

- The Image Manipulation Trace Feature Extractor is a feature extraction network for the purpose of classifying images that have been altered, and it encodes the altered image in a patch into a feature vector with a fixed dimension.
- The Local Anomaly Detection Network is a network that was created with the understanding that in order to effectively detect various types of forgeries, we must evaluate our extracted characteristics more and more locally.

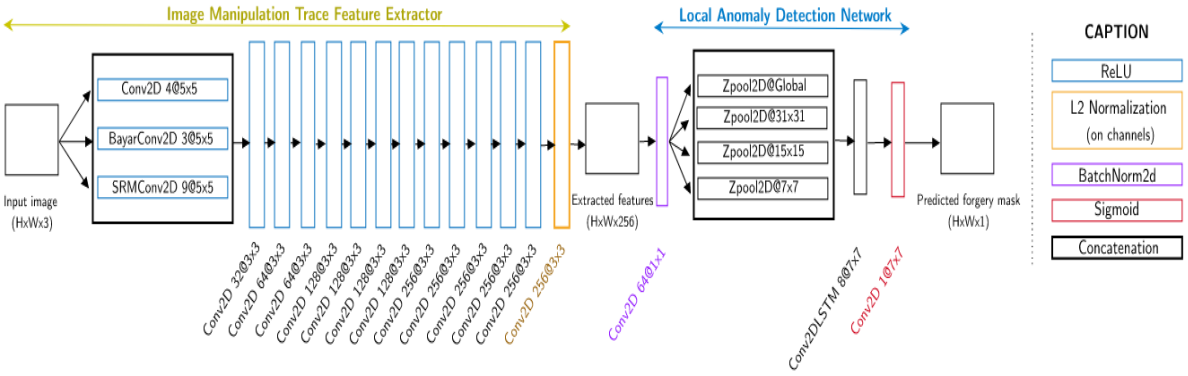


Figure 3.3.4: ManTraNet Architecture

3.4 SELF-CONSISTENCY LEARNING

3.4.1 INPUT IMAGE PREPROCESSING AND CONSISTENCY MAP EXTRACTION

The image is loaded from the specified input directory and the RGB channels are converted to GBR format as OpenCV reads the images in GBR format. The image is then normalised to restrict the pixel values between 0 and 1.

For the ease of processing these images by the pre-trained Siamese Network, the dimensions of the image are ‘unsqueezed’ from (w, h, 3) to (1, 3, w, h) so that it can easily pass through the model. The stride size is dynamically calculated based on the image dimensions. A patch-sized sliding window having the determined stride size is applied over the image to get patches of size 128 x 128. Then, all the consistency maps are generated by comparing each patch in the first patch list with each patch in the second patch list. These maps show relative values to the first patch.

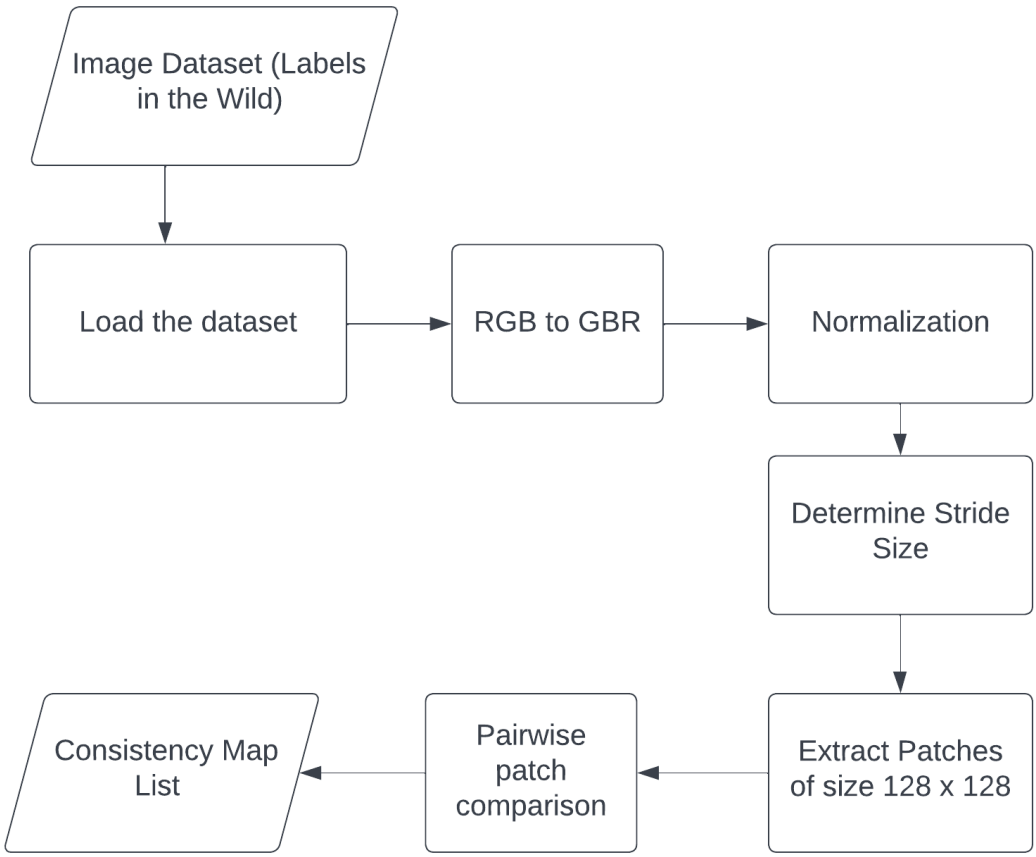


Figure 3.4.1: Input Preprocessing and Consistency Map Extraction

3.4.2 ResNet

A Siamese network is used to predict the probability that a pair of 128 × 128 image patches shares the same value for each EXIF metadata attribute.It uses shared ResNet50 sub-networks, which have been pretrained. Each of the sub-networks produce a 4096-dimension. feature vector. These vectors are concatenated and passed through a multilayer perceptron (4 layers) with 4096, 2048, 1024 units, followed by the final output layer. The network predicts the probability that the images share the same value for each of the n metadata attributes.

ResNet is classic neural network used.Here ResNet50 is used.It is a predefined model which can be imported from pytorch models.And it can be trained to predict the output.

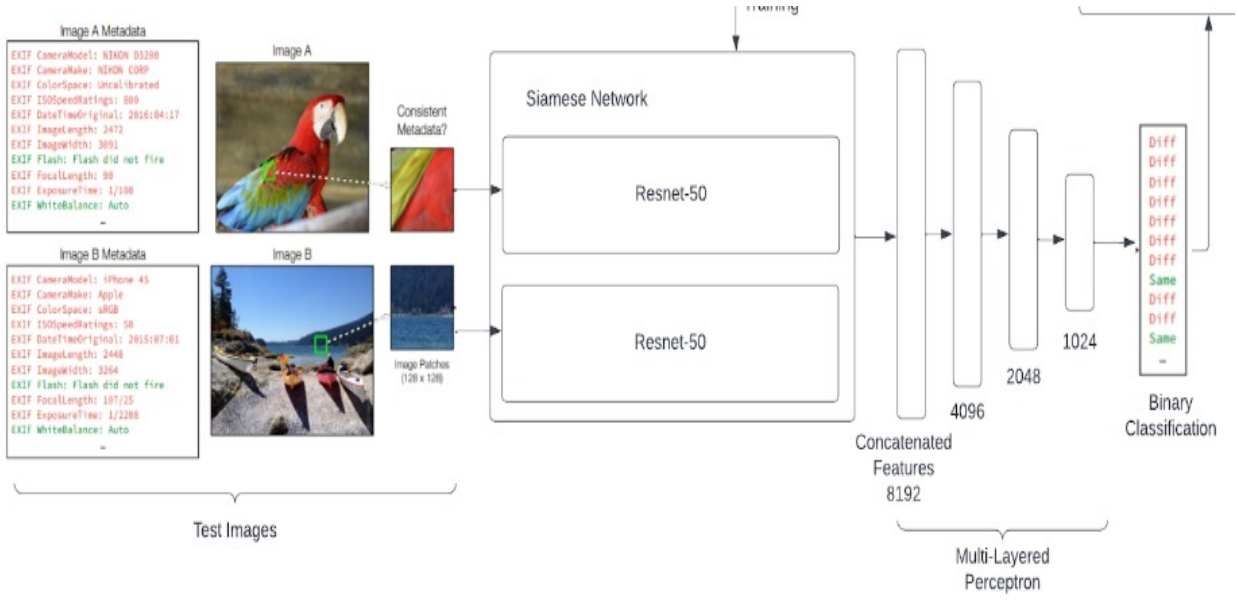


Figure 3.4.2: ResNet

3.4.3 IMAGE SEGMENTATION USING MEAN SHIFT AND NORMALIZED CUT

This module deals with the segmentation of an image into two parts(original and spliced). After the consistency maps for two patches in an image for all EXIF attributes are returned, the points in the resultant map are plotted and the mean shift is calculated.

For the mean shift, points within the 10th percentile for distance from an individual point are considered. Similarly, the resultant map serves as an input for the normalized cut computation that makes use of the sklearn spectral clustering function to return the fit. If most of the image is of high probability, it is flipped.

Finally, the results for mean shift and normalized cut are resized (enlarged) and returned. The interpolation type is Inter Linear of the cv2 package. A sample output has been shown below:

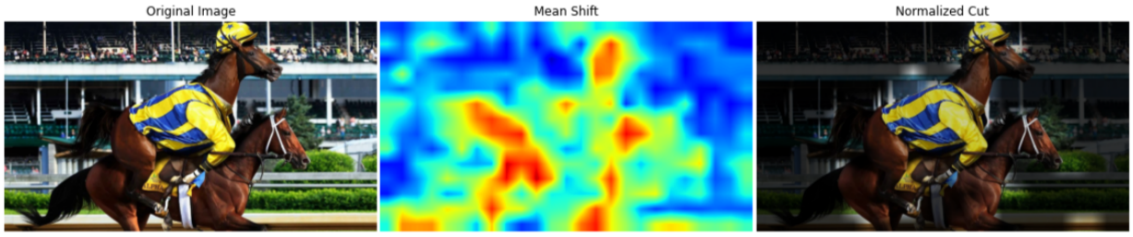


Figure 3.4.3: Localization of tampered region

CHAPTER 4

IMPLEMENTATION OF YOUR WORK

4.1 CNN APPROACH

Algorithm 4.1 Image Patch extractor

Input :input_path,output_path,patches_per_image,no_of_rotations,stride
Output :Rotated image patches

1: START
2: **for** each image in Tampered Images and Authentic Images **do**
3: Apply patch-sized sliding window of stride 128
4: **if** image belongs to Tampered Images **then**
5: Determine tampered patches where num_zeros ¡= 0.99 * (num_zeros + num_ones)
6: **end if**
7: Augment the patches by rotating them by 0, 90, 180 270 degrees.
8: GOTO 2
9: **end for**
10: Store the extracted patches in separate directories for authentic and tampered classes.
11: STOP

Algorithm 4.2 Feature Extraction and Forgery Classification

Input :128x128x3 image patches
Output :1 or 0 (Binary Classification)

1: START
2: The patches are fed into the CNN model, which extracts a 400-D feature representation for each patch.
3: The (n x 400-D) feature representations for an image must be fused into a single feature vector
4: These features are then passed to a fully-connected layer with a 2-way softmax classifier in the training phase and the SVM model in the testing phase.
5: The SVM model returns 1 if the image is tampered, and 0 otherwise.
6: STOP

4.2 UNSUPERVISED SELF-CONSISTENCY LEARNING

Algorithm 4.3 Input preprocessing and consistency map extraction

Input :Test Images
Output : Consistency Map List

1: START
2: Load the images to be tested.
3: Convert RGB to GBR colour scheme.
4: Unsqueeze the image's dimensions from (w, h, 3) to (1, 3, w, h).
5: Calculate stride size based on the image dimensions.
6: Apply patch-sized sliding window to extract patches of size 128 x 128.
7: Compare the obtained patches pairwise and get the probability score of consistency.
8: Obtain the consistency map list.
9: STOP

Algorithm 4.4 Image Segmentation

Input : Image,Image_Patches
Output : Segmented Images using Mean Shift and Normalized Cut

1: START
2: Compute the consistency map of a patch with respect to other patches considering each metadata attribute independently.
3: The resultant consistency map is used to plot the mean shift, taking the top 10 percentile of nearest points into consideration for a given point.
4: The normalized cut is obtained from the consistency maps using the spectral clustering method.
5: If most of the image is high probability, flip it.
6: The resultant images for mean shift and normalized cut are resized, showing the segments clearly.
7: STOP

CHAPTER 5

RESULTS AND PERFORMANCE ANALYSIS

This chapter contains the final output screenshots and performance analysis of this project - A Deep-Learning approach for detecting splicing & copy-move image forgeries and image self-recovery.

5.1 CNN APPROACH

5.1.1 CNN - EPOCH VS TRAINING ACCURACY

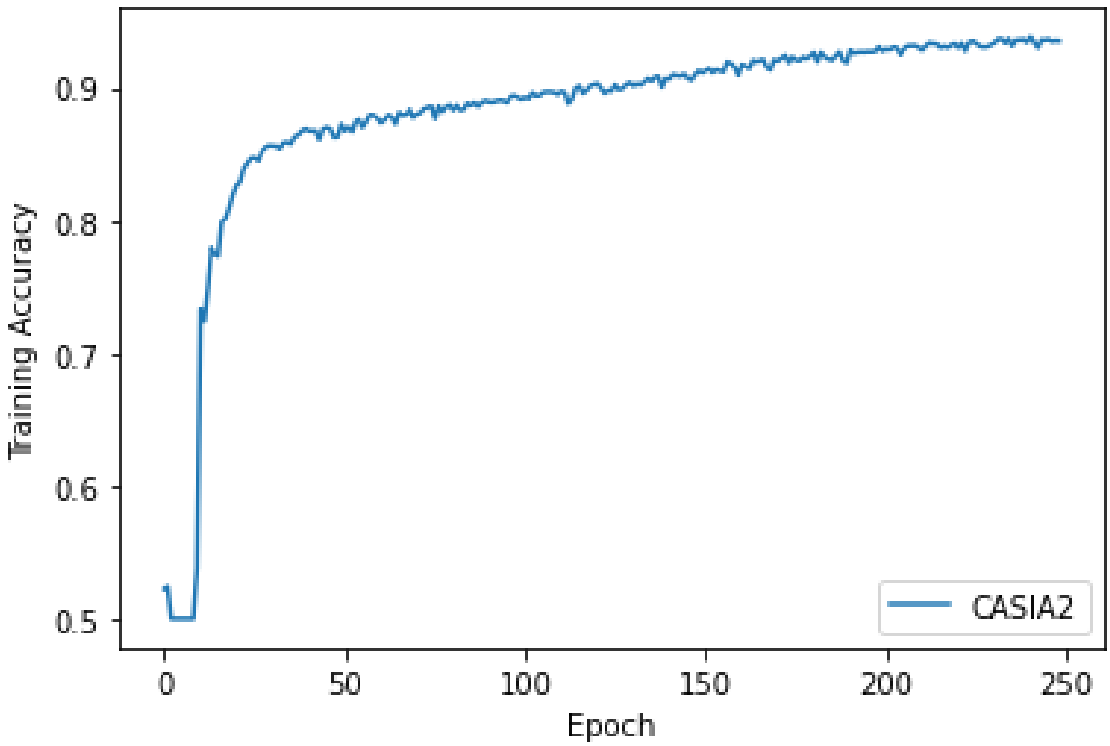
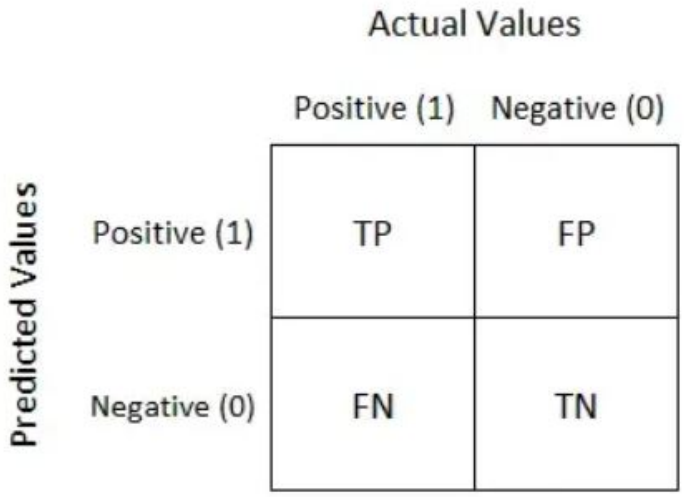


Figure 5.1.1: EPOCH VS TRAINING ACCURACY

As from the graph we can infer that as the Epoch increases the training accuracy also increases and reaches a saturation after which the training accuracy doesn't change much. So the number of epoch is stopped at 250 to prevent overfitting.

5.1.2 SVM PERFORMANCE



A confusion matrix is a tabular summary of the number of correct and incorrect predictions made by a classifier. It is used to measure the performance of a classification model. It can be used to evaluate the performance of a classification model through the calculation of performance metrics like accuracy, precision, recall, and F1-score.

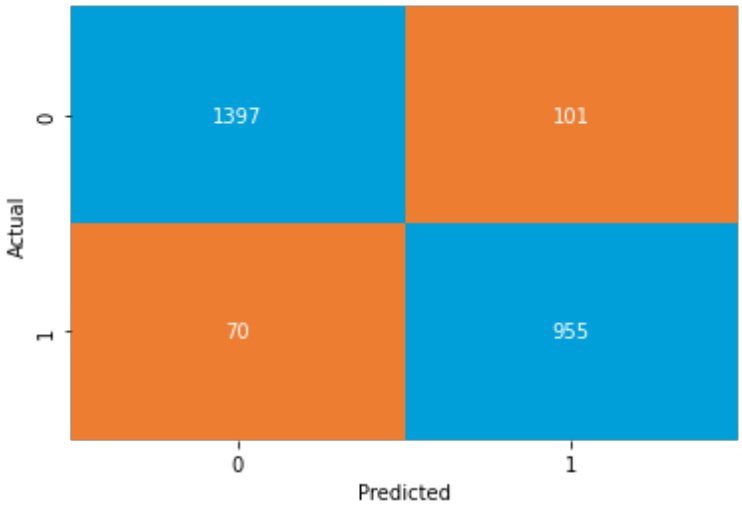


Figure 5.1.2: CONFUSION MATRIX (Testing on 20% of the dataset)

TP -Image is tampered and predicted as tampered

FP -Image is authentic but predicted as tampered

TN -Image is authentic and predicted as authentic

FN -Image is tampered but predicted as authentic

SVM performs binary classification. 0 indicates that the image is authentic and 1 indicates that the image is tampered.

PRECISION : Precision is defined as the ratio of correctly classified positive samples (True Positive) to a total number of classified positive samples. Our model has 90.43% of precision which depicts that almost 10% of tampered images are misclassified as original.

$$\text{Precision} = \frac{TP}{TP+FP}$$

RECALL : The recall is calculated as the ratio between the number of Positive samples correctly classified as Positive to the total number of Positive samples. The recall of our model is 93.1 so it means that 93.1% of tampered images are predicted correctly by our model.

$$\text{Recall} = \frac{TP}{TP+FN}$$

SPECIFICITY : Specificity is the metric that evaluates a model's ability to predict true negatives of each available category. In accordance to our project it refers to the percentage of original images predicted correctly.Our model has a specificity of 93.25%.

$$\text{Specificity} = \frac{TN}{FP+TN}$$

F1 SCORE : The F1 score is defined as the harmonic mean of precision and recall. It is one of the most important evaluation metrics in machine learning. The F1 score of the model is 91.74%.

$$\text{F1} = \frac{2*Precision*Recall}{Precision+Recall} = \frac{2*TP}{2*TP+FP+FN}$$

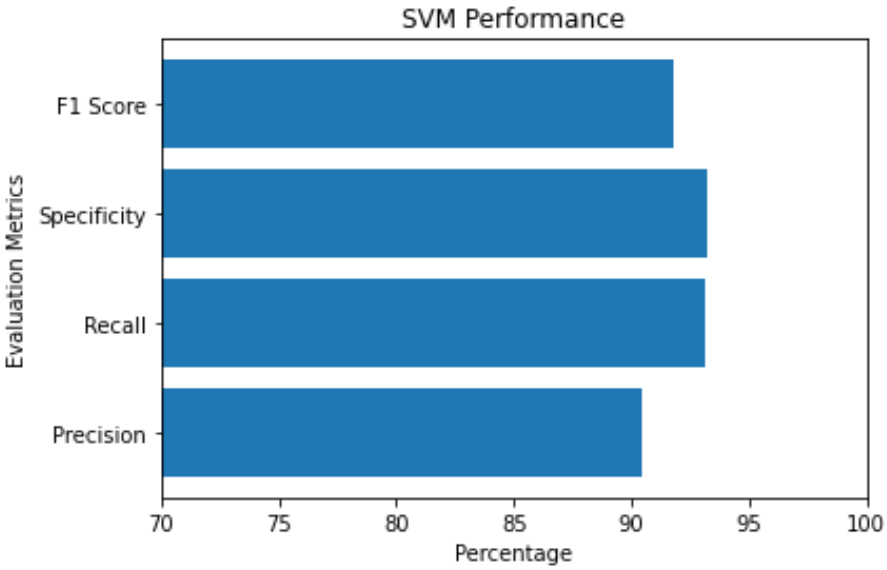


Figure 5.1.3: SVM PERFORMANCE METRICS

5.2 SELF CONSISTENCY LEARNING

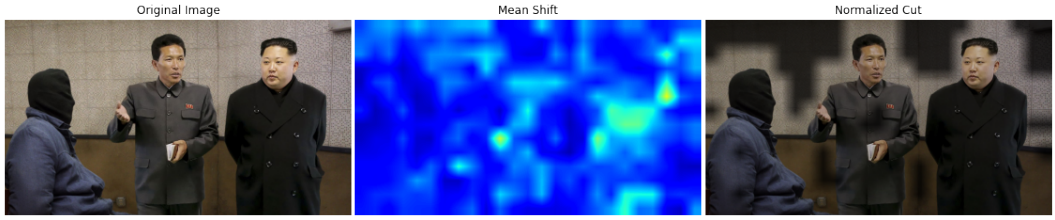


Figure 5.2.1: OUTPUT 1

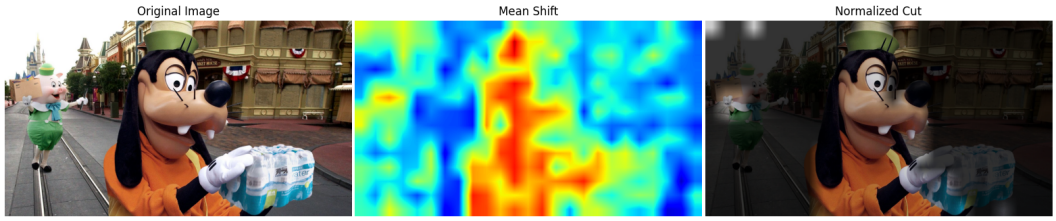


Figure 5.2.2: OUTPUT 2

Fig 5.2.1 and 5.2.2 shows the outputs of Self consistency learning approach.The original image has been followed by its corresponding Mean shift and Normalized cut based segmentation.

5.3 USER INTERFACE

The UI of the project is made using Streamlit, an open-source library available in python. Fig 5.3.1 is a screenshot of the web application developed. The web app prompts the user to upload an image for testing. On image upload, the web app runs the deep learning model in the background to localize the exact region of tampering, if any in the uploaded image. Fig 5.3.1 shows a sample output of the same.

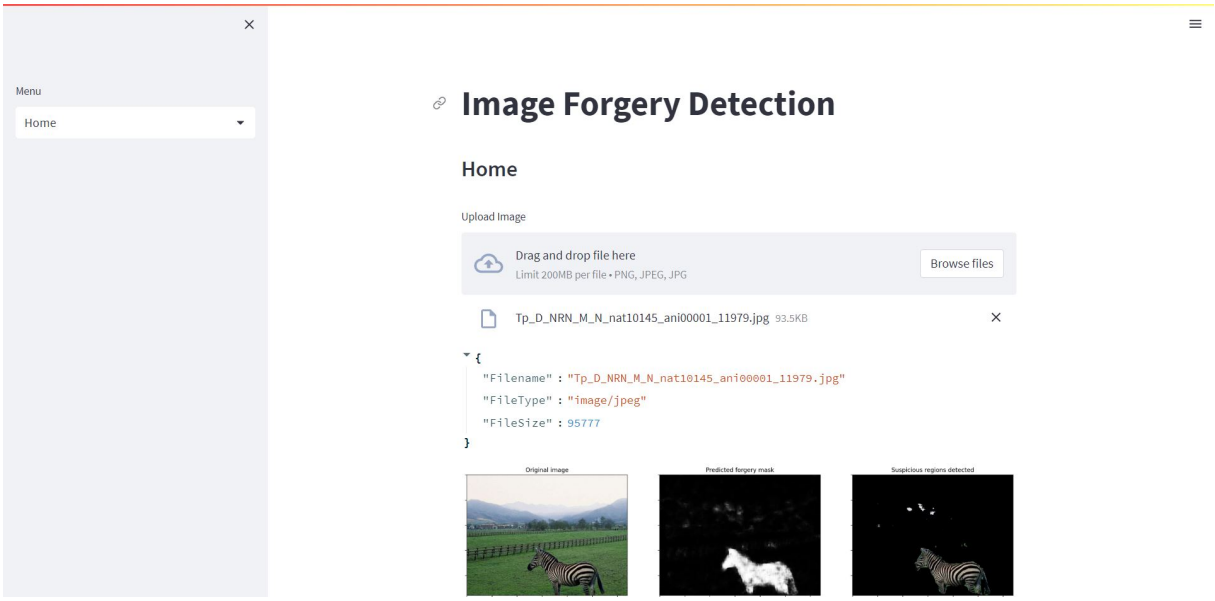


Figure 5.3.1: Tampering Localization in UI

REFERENCES

[1] Mortda A.M. Fouda M.M. Hosny, K.M. and Lashin. An efficient cnn model to detect copy-move image forgery. 2022.

[2] Shaikh M. Gulhane A. Mallick, D. and Maktum. Copy move and splicing image forgery detection using cnn. 44:03052, 2022.

[3] Y. Rao and J. Ni. A deep learning approach to detection of splicing and copy-move forgeries in images. *IEEE international workshop on information forensics and security (WIFS)*, pages pp. 1–6, 2016.

[4] Liu A. Owens A. Huh, M. and A.A. Efros. Fighting fake news: Image splice detection via learned self-consistency. *In Proceedings of the European conference on computer vision (ECCV)*, pages pp. 101–117, 2018.

[5] Bhavsar A. Kumar, A. and R. Verma. Forgery classification via unsupervised domain adaptation. *In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*, pages pp. 63–70, 2020.

[6] Qian Z. Zhou H. Xu H. Zhang X. Ying, Q. and S. Li. From image to imuge: Immunized image generation. *In Proceedings of the 29th ACM international conference on Multimedia*, pages pp. 3565–3573, 2021.

[7] W. AbdAlmageed Y. Wu and P. Natarajan. Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages pp. 9535–9544, 2019.