Jahangirnagar University

Final Year Project Report

A Machine Learning-based Image Forgery Detection

Alif Al Hasan
Mehedi Hasan

Department of Computer Science & Engineering

Supervised by
Asst. Prof. Mohammad Ashraful Islam

May 13, 2023

Abstract

With the availability and usefulness of image manipulation tools, the ubiquity and complexity of identifying picture forging assaults like copy-move and splicing have grown. These kinds of fake digital images are created using clever cropping methods. An automated picture forgery detection system based on machine learning is set up to spot fabricated photos based on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT). Using 2D DCT in LBP space, the chrominance component of the input image is used to extract local features having discriminative qualities. Support vector machines, sometimes known as SVMs, are used for detection. Our system has shown great performance on three picture forgeries datasets (CASIA 1.0, CASIA 2.0, Columbia).

Keywords: DCT, SVM, LBP, copy-move forgery, splicing forgery.

Table of Contents

List of Figures

List of Tables

Acknowledgement

We appreciate our project manager's sage advice and kind cooperation as we finished the assignment. This project could not have been completed on time without his willingness, promptness, and—most importantly—faith in us. Additionally, we would like to convey our gratitude to all of our outstanding teachers from the Department of Computer Science & Engineering at Jahangirnagar University for their important guidance, instruction, and direction during our undergraduate studies and the completion of this project. The direction and mentoring provided by our supervisor have been crucial in helping us shape our project and make sure it adheres to the highest standards. He has been friendly, considerate, and generous with his time, always ready to listen or offer counsel. We have been motivated to pursue our own objectives and aim for excellence in whatever we do by the teachers' relentless dedication to teaching and research. We sincerely appreciate their encouragement and assistance. Our expertise and skills in this subject have grown as a result of their mentoring and coaching. We are grateful for the chance to work under their direction, and we are assured that we are ready to face the difficulties that lie ahead.

Chapter 1

Introduction

1.1 Overview

Since digital photographs can effectively convey a variety of sorts of information, they have become a common component of our daily lives.We can collect large amounts of images thanks to the quick development of cameras and other image acquisition technologies, and the quick development of memory devices made it possible for us to store them. Digital photographs are utilized for a variety of things, from family portraits to scientific study and medical imaging. They provide a concise and practical means of information transmission. They are regarded as the media that conveys information the most effectively. Digital image file formats include TIFF, GIF, JPEG, PNG, BMP, Post-Script, and many others.

1.2 Motivation

Tools for modifying photos that are easy to use include GIMP, Adobe Photoshop, Pixlr, Canva, Inkscape, Fotor, Snapseed, and more. Digital photographs can now be easily altered because they are available across all platforms, which puts a serious threat to their legitimacy. Digital photos may now be used very easily to conceal sensitive information, create obscene graphics, and spread false information on social media and other electronic platforms. These factors have made the need for image fraud detection systems to establish the veracity of digital photographs vital.

1.3 Problem statement

We have to determine whether or not a digital image has been altered in this situation. Digital photographs can be manipulated or altered by experts in image editing without leaving any evident signs of the alterations. To identify forgeries, such as copy-move or splicing forgeries, which are the most frequently employed, our system must examine the properties of the image. Some people manipulate photos to spread false information or to conceal important details in an effort to pique their own curiosity. The original image must remain unchanged by our detection system. Our system ought to be effective and able to quickly analyze a lot of photos. It should be resistant to altered region shapes and different types of forgeries. With a high degree of accuracy, it should be able to tell the difference between real and fake photos. **Local Binary Pattern (LBP)** and **Discrete Cosine Transform (DCT)** is appropriate for feature extraction and **Support Vector Machine (SVM)** ought to be applied for detection. The system must have an intuitive user interface that makes it simple for users to upload and check photographs for possible manipulation.

1.4 Related Works

1. The article "Passive detection of image splicing and copy-move forgery using DCT and LBP" was published by Muhammad Usman et al. in 2017. Using a combination of DCT and LBP features and SVM classification, the suggested technique achieved an accuracy of 97.6% on the CASIA v2.0 dataset.

2. The article "A Comparative Study of Image Forgery Detection Techniques" by Deepak Kumar et al. (2018). In this work, various active and passive methods for detecting image forgeries are compared, and their effectiveness is assessed using data from various datasets. Results demonstrate that passive methods outperform active methods, with some obtaining accuracy rates above 90%.

3. "Forgery detection in digital images using statistical features and machine learning algorithms" is a 2020 paper by M. M. El-Zeiny et al. The suggested technique detects image forgeries by combining machine learning methods like KNN and SVM with statistical variables like mean, variance, and skewness. On a dataset of 500 photos, the technique had a 96% accuracy rate.

4. Hafiz M. Asif and colleagues published "Deep learning-based forgery detection in digital images" in 2018. A convolutional neural network (CNN) is used in the proposed method's deep learning model to identify fake images. On 900 photos in the dataset, the approach had a 98.5 percent accuracy rate.

5. Qingzhong Liu et al.'s study "A survey of deep learning-based image forgery detection techniques" was published in 2019. Several deep learning-based image forgery detection methods, including CNNs, autoencoders, and generative adversarial networks (GANs), are reviewed and assessed in the survey. The findings indicate that CNN-based techniques perform the best, with some of them obtaining accuracy rates above 99%.

6. Shihao Zhang et al. (2019) published a study titled "Forensic detection of image tampering using deep convolutional neural networks." The suggested method analyzes a picture's noise residuals using a deep CNN to find evidence of image alteration. On the COVERAGE dataset, the approach had an accuracy rate of 98.4%.

7. A study by Shangzhen Luan et al. (2018) titled "Passive detection of image forgery using scale-invariant feature transform and support vector machine" was published. The suggested technique employs SVM classification and scale-invariant feature transform (SIFT) to identify fake images. On the CASIA v1.0 dataset, the technique has an accuracy rate of 94.6 percent.

8. The article "Detecting copy-move forgery in digital images using normalized radial projection" was published in 2017 by W. Khemakhem et al. In order to identify copy-move forgeries in digital images, the suggested method employs normalized radial projection (NRP). On a dataset of 120 photos, the approach had a 97.5 percent accuracy rate.

9. R. A. Javed et al.'s paper "A forensic approach for copy-move forgery detection based on clustering and local binary pattern" was published in 2019. The suggested method detects copy-move forgeries in digital photos by combining clustering and local binary pattern (LBP) features. On a collection of 250 photos, the approach had a 95.3% accuracy rate.

10. The article "Image tampering detection using adaptive histogram equalization and support vector machine" was published in 2018 by Pranav Kumar Singh et al. The suggested method employs SVM classification and adaptive histogram equalization (AHE) to identify altered images. On a dataset of 300 photos, the approach had a 96.6 percent accuracy rate.

Image forgery detection has improved more swiftly than image forgery-type identification, according to the literature that is now available. This has a great deal of potential for providing authenticity for digital images.

1.5 Aim and objectives

Our goal is to create an accurate and reliable picture forgery detection system that can determine whether an image has been altered or manipulated and what kind of counterfeit it is.The image forgery detection system has the following specific goals:

1. The creation of a system that can recognize many kinds of image frauds, including copy-move and splicing.

2. Building a system that can process massive quantities of photos and is accurate and efficient.

3. putting into practice cutting-edge algorithms and methods to increase the system's accuracy and robustness.

Generally speaking, the purpose and goals of creating an image forgery detection system that can help in the detection and prevention of image manipulation and forgery.

1.6 Scope and limitations

Systems for detecting different kinds of image forgeries can be used in a wide variety of applications. Their accuracy and resilience can be increased with more sophisticated algorithms and methods. Both static and moving graphics can be used with our system. Systems for detecting picture forgeries can also be used to locate the origin of modified images and find the origin of image forgeries. Because image fraud is becoming more prevalent, it is expected that the range of image forgery detection systems will continue to grow in the future.

When an input image has poor illumination or low resolution, our image fraud detection system performs with only a limited degree of effectiveness. To avoid detection, many cutting-edge picture alteration techniques have emerged. In the detection process, false positives and false negatives might happen, which can lower the system's overall reliability. In real-time or close to real-time settings, our approach might not be successful in spotting forgeries.

1.7 Report Layout

Here's a quick summary of the report's structure:

- Chapter 1 provides a summary of the goals. Here is where the purpose of the project is described. The problem's definition is also looked at. The type of effort that has already been done in this subject is another consideration. the system's goals and objectives in development. Here, we also talk about the system's scope and constraints.

- The Chapter 2 of this project's literature list includes works we have read both before and during its creation.

- In Chapter 3, we examined datasets, a suggested model, feature extractions, and methods and flowcharts. The main architecture of the project is the subject of this chapter.

- In Chapter 4, the findings and analysis are covered.

- The conclusion, which includes a summary of the project, is the last section we examine in Chapter 5. Additionally, we take future work into account.

Chapter 2

Literature review

- Alahmadi et al. [1] (2018) a study was done and a new strategy for detecting picture fraud using the discrete cosine transform (DCT) and local binary pattern (LBP) techniques was developed. They put forth a technique that extracts frequency components and texture features, using the information to train a support vector machine (SVM) classifier to determine whether or not an image is fake. They tested their technique on a dataset of 800 photos, and their system had an accuracy of 98.5%, suggesting that the technique is effective in identifying different kinds of image fraud.

- Parnak et al. [2] (2020), using the basis of both generalized and conventional Benford's Law, a unique technique for detecting picture splicing was proposed. This program extracts features from a picture using the logarithmic distribution of first and higher-order digits technique. On a benchmark dataset, they assessed the algorithm's performance, and after comparison, they discovered that the suggested algorithm performed better than other well-known algorithms already in use. In the future, this method might be used in systems with a lot of users. Comparatively to many cutting-edge algorithms, it has a much higher success rate.

- Manzarul et al. [3] (2017) for the purpose of identifying copy-move and splicing assaults in their article, persented a reliable forgery detection method. Splicing and copy-move are two frequent types of picture fraud techniques that might be challenging to spot. Scale-invariant feature transform (SIFT) and discrete cosine transform (DCT) approaches are the foundation of their algorithm. To extract features from the image, the DCT is employed. The assault area is then determined by matching them using SIFT. To increase the detection accuracy and resilience, the algorithm combines the two well-known algorithms DCT and SIFT. Several datasets were used to assess the performance of the suggested technique, which demonstrated extremely good accuracy.

- Shilpa et al. [4] (2016) has developed a method that makes use of block discrete cosine transform (DCT) coefficients' statistical properties. This technique makes it easier to determine whether or not an image block is fake. With this technique, the input image is divided up using block-wise DCT. the DCT coefficients are then used to obtain statistical characteristics. Finally, depending on the retrieved features, determine if the photographs are fake or not. The experimental outcomes demonstrated very good accuracy, and the authors assessed their method using some well-known datasets. Their suggested approach demonstrated the possibility for large-scale practical implementations of image forgery detection systems based on statistical aspects of block DCT coefficients.

- Mahmood et al. [5] (2020) in their study titled ”A Survey on Block Based Copy Move Image Forgery Detection Techniques,” the authors present a thorough survey of several methods used to identify block-based copy-move image fraud. The techniques were divided into four primary groups by the authors, who also provided a thorough analysis of their advantages and disadvantages. On the basis of several evaluation measures, they also compared the effectiveness of the various strategies. This essay provides details on the precision and restrictions of each method. The study makes the case for the possibility of integrating various methodologies to produce outcomes that are more precise and trustworthy.

- Soumen et al. [6] (2015) in their study ”Copy-Move Image Forgery Detection using SVD,” they suggested a technique to identify copy-move forgeries in digital photographs. In the suggested method, an image is first broken down into its component parts using SVD, and then comparable image patches are grouped together using a clustering algorithm. The approach then compares how similar each pair of patches in a group are to one another in order to find the duplicated region. On a few widely used datasets, they assessed how well this strategy performed.

- Mohammed et al. [7] (2018) in their publication, ”Detection of copy-move image forgery based on discrete cosine transform,” the authors suggested a method to identify copy-move image fraud using the discrete cosine transform (DCT). A clustering algorithm is then used in the proposed method to group comparable characteristics after using DCT to extract features from the image. The duplicated portions within the image are then found by comparing the features that were grouped. On some very well-known datasets, they tested this method's performance, and it performed admirably.

Chapter 3

Background Technologies

3.1 Discrete Cosine Transform (DCT)

Discrete Cosine Transform, or simply DCT, is a well-liked method for compressing and analyzing images. A set of frequency coefficients are created from an image using DCT. The energy content of the image can be represented in various frequency bands using these frequency coefficients. DCT is frequently used in image forgery detection to spot areas that have been altered by copy-move or splicing operations. DCT is utilized for lossy image compression due to its extremely powerful energy compaction. A block of an 8 × 8 matrix must be created from the input image in order to execute DCT on it. After that, we do a discrete cosine transform on the data block. The discrete cosine transform (DCT) aids in delineating the various spectral bands within the image. The fundamental formula for a 2D (N by M picture) DCT is:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} \Lambda(i).\Lambda(j).cos\left[\frac{\pi.u}{2.N}(2i+1)\right] cos\left[\frac{\pi.v}{2.M}(2j+1)\right].f(i,j)$$

where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

Simple Cosine Data points in a spatial domain are converted via transform into frequency domain data points. This makes it simpler to identify repeated patterns.

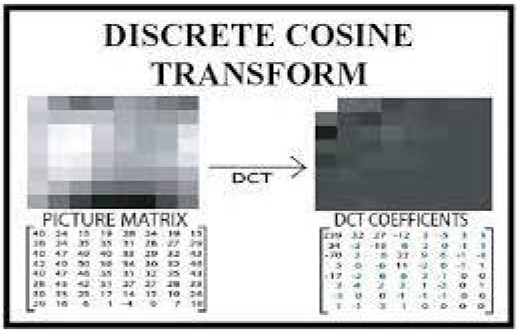
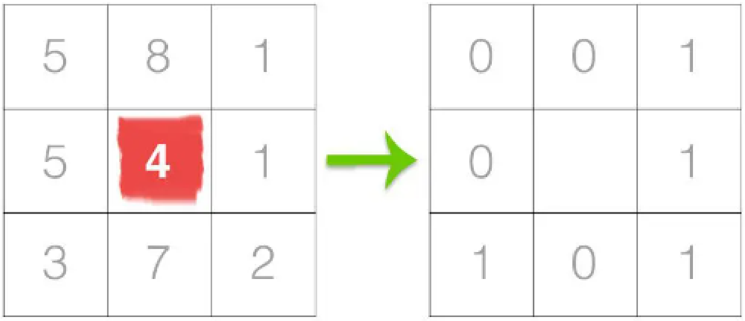


Figure 3.1: Discrete Cosine Transform
[8]

3.2 Local Binary Pattern (LBP)

LBP, or local binary pattern, is a technique for examining texture in photographs that generates a binary code for each pixel based on comparisons between its intensity and that of the pixels around it. By spotting changes or inconsistencies in an image's texture, LBP is widely used to spot image fraud. Following the release of an article by Ojala et al., this method gained widespread recognition. [9] Although the idea of LBPs had been presented as early as 1993, the paper ”Multiresolution Grayscale and Rotation Invariant Texture Classification with Local Binary Patterns” was published in 2002. Using each pixel and its surrounding pixels as a starting point, local binary patterns produce a local interpretation of texture. It is necessary to transform the image to grayscale in order to construct an LBP texture description. The next step is to choose a neighborhood of a given radius (designated as ”r”) around each pixel in the grayscale image. Following that, a value for the center pixel is determined using LBP and recorded in a 2D array with the same dimensions as the original image.

- The procedure of thresholding is used to convert the neighborhood of 8 pixels around the central pixel into a collection of 8 binary digits in the initial stage of creating an LBP.

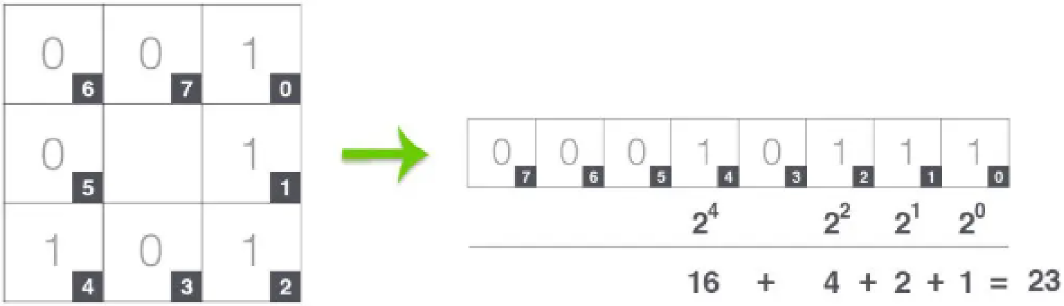


5	8	1
5	4	1
3	7	2

0	0	1
0		1
1	0	1

Figure 3.2: First step of LBP
[10]

- It is crucial to follow a consistent order while evaluating the surrounding pixels in a clockwise or counterclockwise orientation in order to identify the LBP value of the center pixel, and this should be done to all images in our dataset. Using this method, a binary test is used to evaluate the eight adjacent pixels in a 3 × 3 neighborhood. The outcomes of this binary test are saved in an 8-bit array, which is then transformed into decimal form using a technique similar to this:

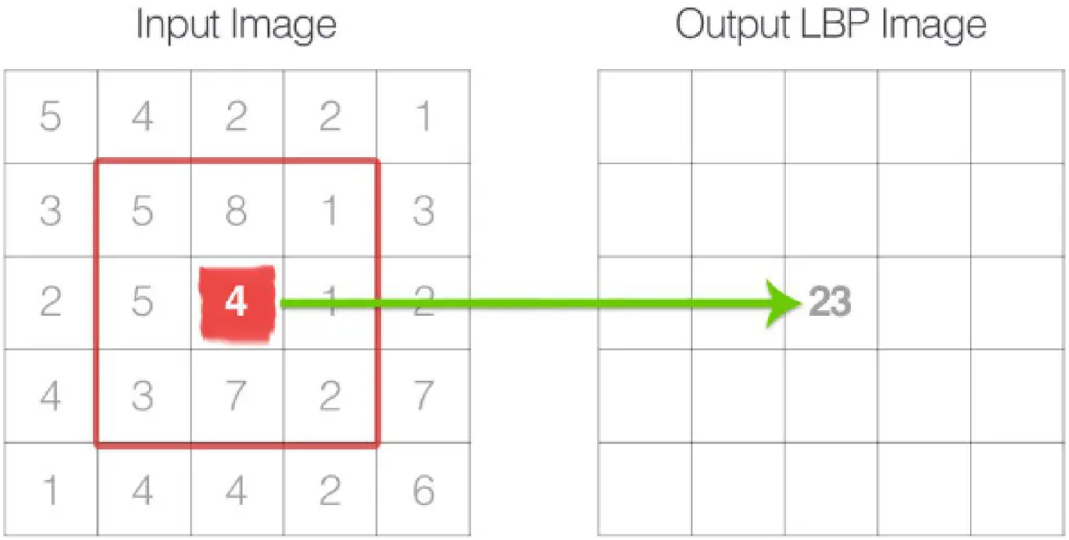


0 6	0 7	1 0
0 5		1 1
1 4	0 3	1 2

7	6	5	4	3	2	1	0
0	0	0	1	0	1	1	1

Figure 3.3: Second step of LBP
[10]

- The computed LBP value is then maintained in an output array with width and height equal to those of the original image.



Input Image

5	4	2	2	1
3	5	8	1	3
2	5	4	1	2
4	3	7	2	7
1	4	4	2	6

Output LBP Image

		23		

Figure 3.4: Final step of LBP
[10]

Each pixel in the input image is then subjected to the aforementioned process, which includes applying a threshold, collecting binary strings, and storing the resulting decimal value in the LBP array.

3.3 Support Vector Machines (SVM)

The well-known machine learning algorithm known as Support Vector Machine, or SVM, is utilized for classification. Its main objective is to identify the best decision boundary for separating the many categories that are available in a dataset. SVM is widely used to categorize photos as genuine or altered based on the features that have been extracted in image forgery detection. Supervised machine learning (SVM) is a type of model. In this approach, each data point is represented as a point in n-dimensional space (where 'n' denotes the number of attributes), and the value of each feature is associated with a particular position. The classification is carried out by locating the hyperplane dividing the two categories. For the classification of our data, we used the SVC linear kernel and polynomial kernel modules. When the data can be divided into equal halves along a single line, it is said that the linear kernel is being used. One of the most used kernels, it is especially helpful for datasets with high dimensionality. A more inclusive representation of the linear kernel is the polynomial kernel, on the other hand. In a feature space over polynomials of the kernel's initial variables, it shows how closely spaced out vectors in the training sample are. The reason this kernel is not as popular is because it is less accurate and effective than the linear kernel.

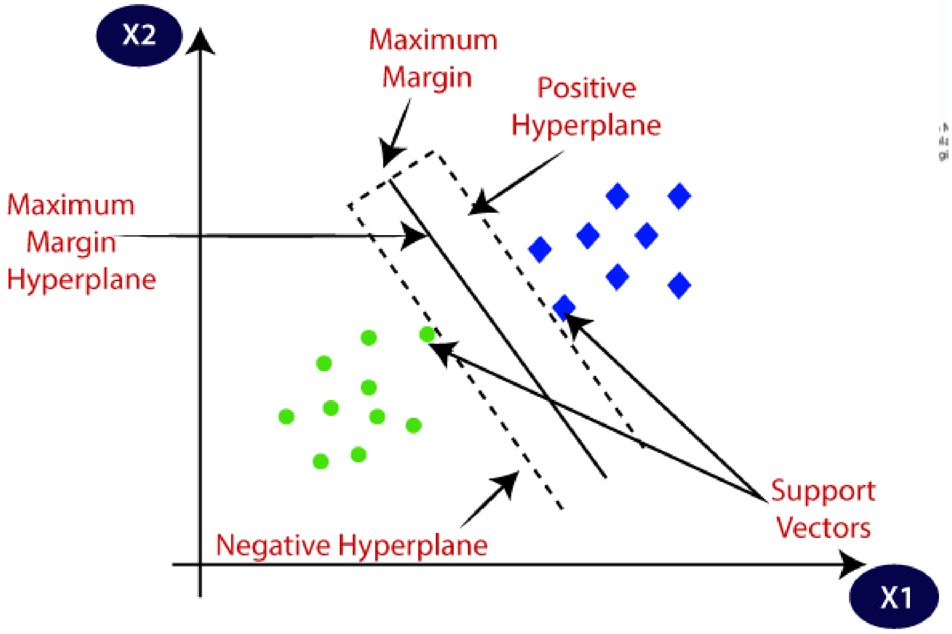


Figure 3.5: Working principle of SVM
[11]

Chapter 4

Methodology

4.1 Overview

By simply copying and pasting portions of the image, image tampering—also referred to as copy-move or splicing—can be carried out. Because of these structural changes in the original image, there is a break in continuity along the margins and a change in the microtexture patterns inside and surrounding the pasted region. There is no longer any association between the image pixels in the area as a result of the local frequency distribution changing. The Local Binary Pattern (LBP) operator is appropriate for emphasizing these tampering artifacts and making them more apparent in the original image. Detection of these structural modifications is vital for properly identifying tampering. The following phase entails monitoring modifications to the local frequency distribution of the LBP image. This is accomplished by first employing a block-based discrete cosine transform (DCT) to transform the LBP picture into the frequency domain, and then by collecting statistical measurements of each DCT coefficient over all blocks.

An image forgery detection system often requires solving a binary decision problem to determine if a picture is real or fake. This system needs to pre-process the image in order to extract its features, then it needs to classify the features. It is critical to have a reliable feature extraction technique since the features of an image indicate the statistical and structural changes brought about by manipulation. Our suggested system is mostly focused on this. The collected features are then used as input into a binary classifier, such a machine learning model, to differentiate between real and fake photos.

Preprocessing, feature extraction (which models the tampering traces), and classification are the three key elements of the system's proposed design.

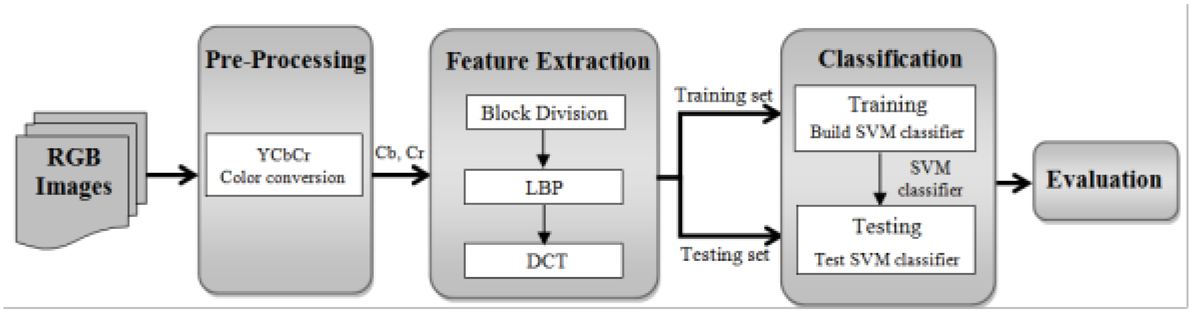
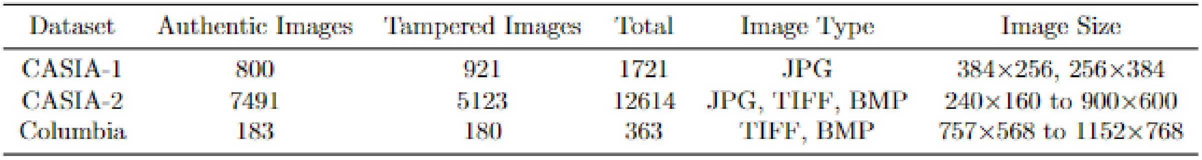


Figure 4.1: System Design of our model
[1]

4.2 Dataset

The suggested system has been evaluated using three benchmark datasets that are well-known in the field. These include the Columbia Image Splicing Detection Evaluation Dataset (Columbia) and the CASIA Tampered Image Detection Evaluation Database Versions 1.0 and 2.0 (CASIA TIDE v1.0 and v2.0), both produced by the Institute of Automation of the Chinese Academy of Sciences. These are collectively referred to as CASIA 2010 and CASIA 2010. These datasets are thought to be more difficult and realistic in terms of manipulation detection. Table 4.1 offers comprehensive details on these datasets.

Table 4.1: Description of the three datasets used in the project



Dataset	Authentic Images	Tampered Images	Total	Image Type	Image Size
CASIA-1	800	921	1721	JPG	384×256, 256×384
CASIA-2	7491	5123	12614	JPG, TIFF, BMP	240×160 to 900×600
Columbia	183	180	363	TIFF, BMP	757×568 to 1152×768

4.3 Proposed Model

4.3.1 Preprocessing

The chroma channels are superior to the other channels at encoding tampering traces. To begin with, the RGB image is converted into a YCbCr image, where Y stands for the luminance component and Cb and Cr are the chroma channels. The majority of the image data is kept in the Y channel in accordance with the YCbCr color model. Therefore, compared to the chroma components, the luminance component is easier for the human eye to distinguish. The majority of tampering traces that cannot be detected with the naked eye are buried in the chroma channels, despite the fact that the human eye is more sensitive to the luminance component. As a result, due to the limitations of human eyesight, altered images may be mistakenly classified as real. Consequently, the chroma channels are essential for spotting tampering. To get around this problem, this study employs all three channels—Y, Cb, and Cr—and combines the derived features from each of the three components to produce a final feature.

4.3.2 Modeling the DCT domain tampering traces

In our system, tampering traces are modeled by LBP and 2D DCT. To aid in localization, a chroma component is originally divided into blocks that have a 50% overlap. The LBP operator is then used to each block to discover instances of micro-patterns and highlight any tampering artifacts that have been added, such as minute edges inside pasted regions and sharp edges along their borders. This technique makes the tampering artifacts in the host picture more pronounced. The next step is to employ 2D DCT to translate each block of LBP codes into the frequency domain in order to detect changes in the local frequency distribution. The standard deviations of the corresponding DCT coefficients are used to construct a feature vector.

Different texture micro-patterns can be distinguished using the local binary operator (LBP). LBP(P,R) represents the LBP operator and stands for:

$$LBP_{P,R} = \sum_{i=1}^{P-1} S(P_i - P_c)2^i$$

where P is the total number of points P(i) in the current pixel Pc's circular neighborhood, which has a radius of R, and the threshold function S(x) is defined as:

$$S(P_i - P_c) = \begin{cases} 1 \; P_i - P_c \geq 0 \\ 0 \; P_i - P_c < 0 \end{cases}$$

To represent tampering traces in the DCT domain, a structured approach is used. An initial 50% overlap block division of a chroma component is performed to aid with localization. After that, each block is put through the LBP operator to highlight and bring to light any tampering artifacts present in the host image. The next step is to translate each block of LBP codes into the frequency domain using 2D DCT, capturing changes in the local frequency distribution. Using the standard deviations of the corresponding DCT coefficients, a feature vector is last but not least produced. Using this technique, it is easier to discover tampering traces. The details of this process are illustrated in the figure below:

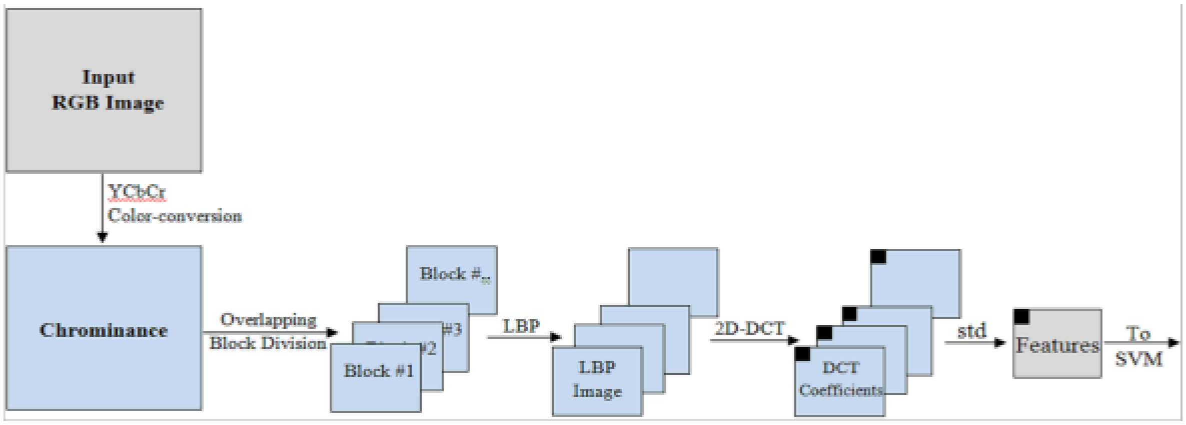


Figure 4.2: Specifics of the modeling procedure for the tampering traces [1]

4.3.3 Classification

The main challenge in image forgery detection is determining if an image is authentic or has been manipulated. Support Vector Machine (SVM), a machine learning technique, has proven to perform exceptionally well in a variety of two-class tasks. Thus, in the given method, classification is performed using SVM and Radial Basis Function (RBF). The SVM classifier defines a perfect hyperplane that separates the data into two categories. The best hyperplane to use to increase the generalization of the classifier is the greatest margin hyperplane, which is the separation between the hyperplane and the nearest samples, referred to as support vectors. The classes are then linearly separable when the data are transferred to a higher dimensional space via SVM and kernel functions.

4.3.4 Evaluation Policy

Machine learning model evaluation is essential because it enables us to compare and choose the model that performs the best for a given task. It offers numerical metrics of performance, assisting us in determining areas in need of improvement and assisting us in making defensible choices on model optimization. Additionally, evaluation determines the model's ability to generalize by projecting its performance on hypothetical data, ensuring its dependability and efficiency in actual situations.

Our model has been assessed in five distinct incorporating the f1-score, precision, recall, cross-validation, and accuracy scores among other assessment methods.

The accuracy score, which is a frequently used performance indicator, computes the proportion of accurately predicted occurrences to all instances. It offers a general evaluation of how accurate the model is. A high accuracy rating means that the model has correctly predicted the outcome. But in the presence of unbalanced datasets, where the proportion of instances in various classes differs noticeably, accuracy can be deceptive. In these circumstances, predicting the majority class is usually sufficient to get a high accuracy score. As a result, it's crucial to take into account other performance indicators.

Cross-validation is a technique used to evaluate the generalization capability of our model. Instead of relying on a single train-test split, cross-validation involves splitting the dataset into multiple subsets or folds. The model is trained on a subset of the data and evaluated on the remaining fold. This process is repeated for each fold, and the performance scores are averaged to obtain the cross-validation score. This approach helps us assess how well our model performs on unseen data and reduces the risk of overfitting or underfitting to a specific train-test split. Commonly used cross-validation techniques include k-fold cross-validation, stratified k-fold cross-validation, and leave-one-out cross-validation.

Precision measures the proportion of correctly predicted positive instances out of all instances predicted as positive. It focuses on the quality of positive predictions and quantifies the model's ability to avoid false positive errors. Precision is calculated as:

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}} \tag{4.1}$$

A high precision score means the model is dependable at spotting positive cases because it has a low rate of false positives.

Recall, sometimes referred to as sensitivity or true positive rate, calculates the percentage of positively anticipated events among all positively occurring events. It emphasizes the completeness of positive predictions and measures the model's accuracy in spotting positive examples. The formula for the recall is:

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \tag{4.2}$$

When a model has a high recall score and a low false negative rate, it is likely to be successful in capturing the majority of positive cases.

The F1 score provides a balanced measurement that considers both precision and recall because it is the harmonic mean of these two variables. As a result, we can evaluate the overall effectiveness of the model because it integrates these two criteria into a single value. The following formula is used to determine the F1 score:

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4.3}$$

The F1 score offers a single statistic to assess the trade-off between precision and recall and takes into account both false positives and false negatives. It is especially helpful when we need to weigh the relative value of precision and recall in the predictions made by our model.

Collectively, these performance indicators offer insightful information about the model's performance and aid in our decision-making when it comes to model comparison, tuning, and selection. When selecting the ideal performance measure(s) to assess our models, it is crucial to take into account the unique traits and requirements of the current issue.

Chapter 5

Results

5.1 Overview

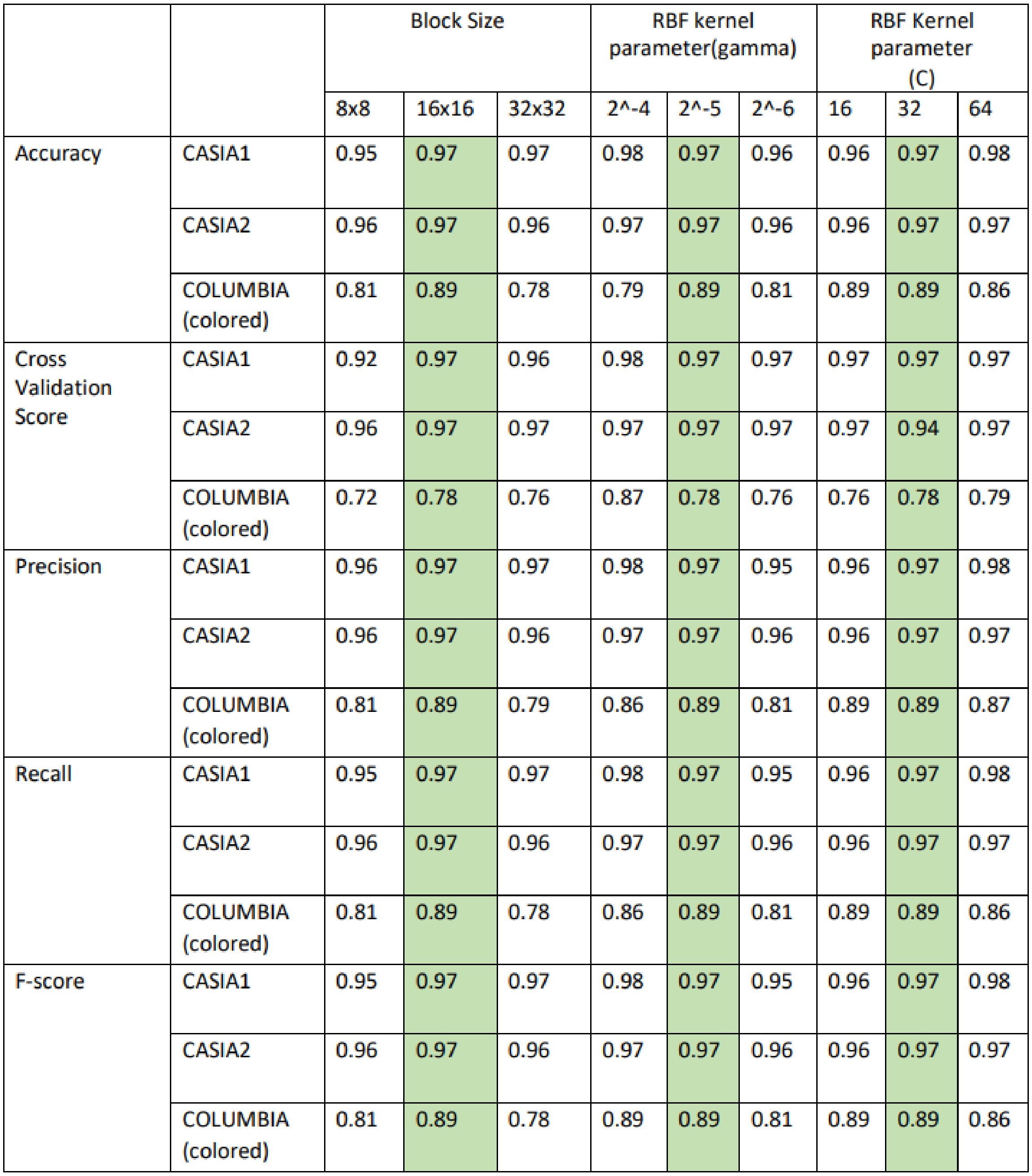
This chapter has two main sections- Section 5.2 Result and Section 5.3 Discussion. In the first section, we will present our findings and project output. In the latter one, we will explain our findings.

5.2 Result

We have split the photos into blocks and computed LBP for each of the blocks in order to categorize an image as legitimate or tampered with. After that, we determined the standard deviation of these data after DCT transformation. To train our model using SVM, these values were utilized as features. Three distinct datasets—CASIA version 1, CASIA version 2, and COLUMBIA (colored)—were used to train our model.

To get the best performance we have tried different tuning on the model such as different block sizes and different values for the parameters of RBF kernel such as - gamma and C. Then we have picked the combination that provides the best result. The following table shows our proposed system's performance on the different setup of parameters mentioned earlier.

Table 5.1: Performances of the model on different setups



		Block Size			RBF kernel parameter(gamma)			RBF Kernel parameter (C)		
		8x8	16x16	32x32	2^-4	2^-5	2^-6	16	32	64
Accuracy	CASIA1	0.95	0.97	0.97	0.98	0.97	0.96	0.96	0.97	0.98
	CASIA2	0.96	0.97	0.96	0.97	0.97	0.96	0.96	0.97	0.97
	COLUMBIA (colored)	0.81	0.89	0.78	0.79	0.89	0.81	0.89	0.89	0.86
Cross Validation Score	CASIA1	0.92	0.97	0.96	0.98	0.97	0.97	0.97	0.97	0.97
	CASIA2	0.96	0.97	0.97	0.97	0.97	0.97	0.97	0.94	0.97
	COLUMBIA (colored)	0.72	0.78	0.76	0.87	0.78	0.76	0.76	0.78	0.79
Precision	CASIA1	0.96	0.97	0.97	0.98	0.97	0.95	0.96	0.97	0.98
	CASIA2	0.96	0.97	0.96	0.97	0.97	0.96	0.96	0.97	0.97
	COLUMBIA (colored)	0.81	0.89	0.79	0.86	0.89	0.81	0.89	0.89	0.87
Recall	CASIA1	0.95	0.97	0.97	0.98	0.97	0.95	0.96	0.97	0.98
	CASIA2	0.96	0.97	0.96	0.97	0.97	0.96	0.96	0.97	0.97
	COLUMBIA (colored)	0.81	0.89	0.78	0.86	0.89	0.81	0.89	0.89	0.86
F-score	CASIA1	0.95	0.97	0.97	0.98	0.97	0.95	0.96	0.97	0.98
	CASIA2	0.96	0.97	0.96	0.97	0.97	0.96	0.96	0.97	0.97
	COLUMBIA (colored)	0.81	0.89	0.78	0.89	0.89	0.81	0.89	0.89	0.86

Evaluating different setups of parameters, we have found that a block size of 16x16 along with RBF kernel parameter gamma = 0.03125 and C = 32, provides the best performance.

In this setup, the CASIA-1 dataset's accuracy is 97.11% and the cross-validation score with 10-fold is 97.09%. Besides it gains a precision value of 0.97, an f-score of 0.97, and a recall value of 0.97. [Figure 5.1]

In the best setup of parameters, the CASIA-2 dataset's accuracy is 96.59% and the cross-validation score is 97.14%. It gains precision, f-score, and recall value each of 0.97.[Figure 5.2]

Following the most accurate setups, COLUMBIA(colored) dataset shows accuracy and cross-validation scores of 89.19% and 77.91% respectively. The system achieves precision, recall, and an f1-score value of 0.89 each.[Figure 5.3]

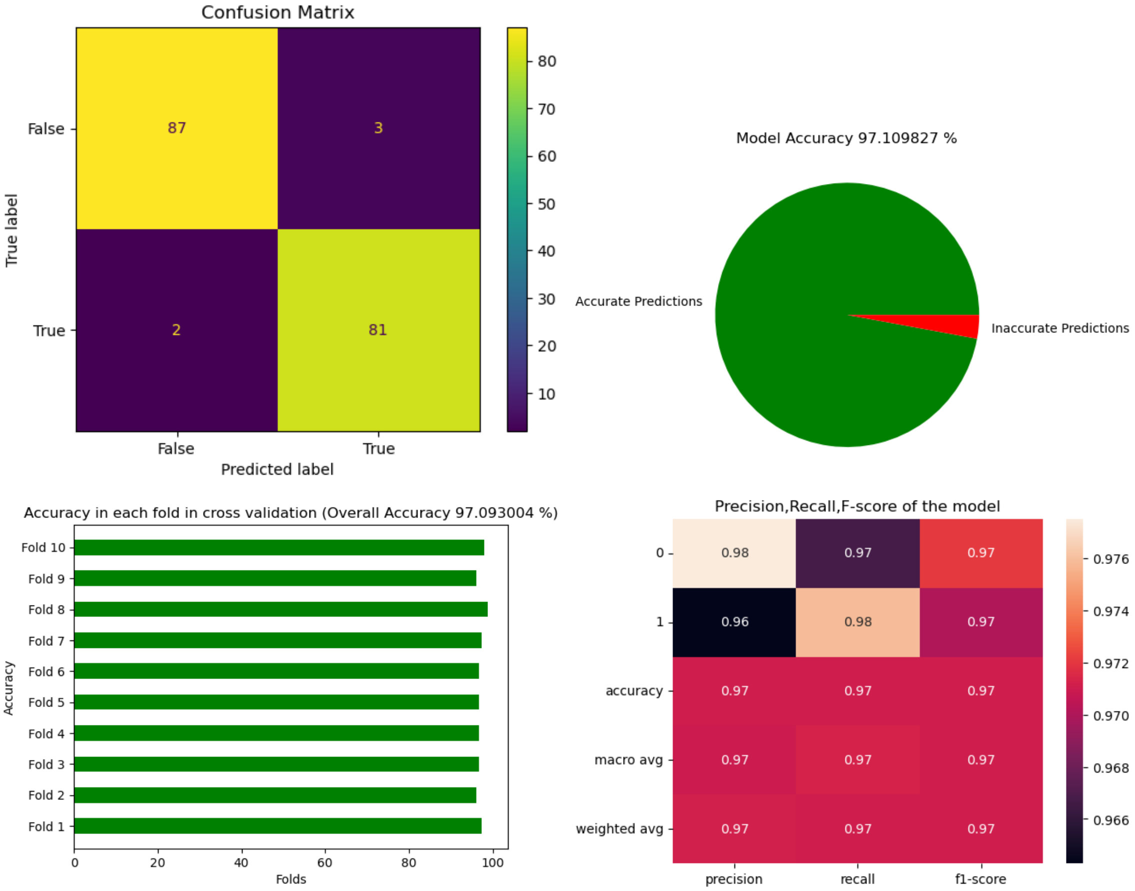


Figure 5.1: Different Performance Measures of CASIA 1 dataset

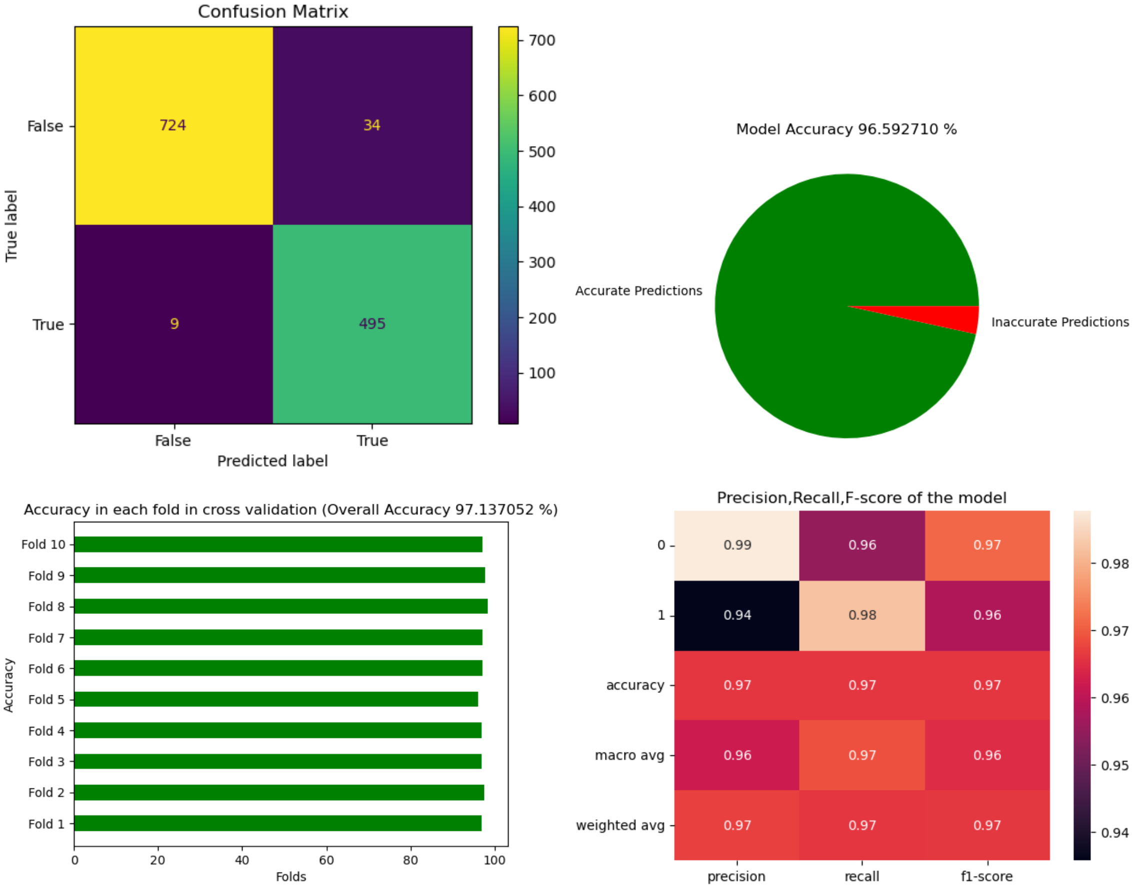


Figure 5.2: Different Performance Measures of CASIA 2 dataset

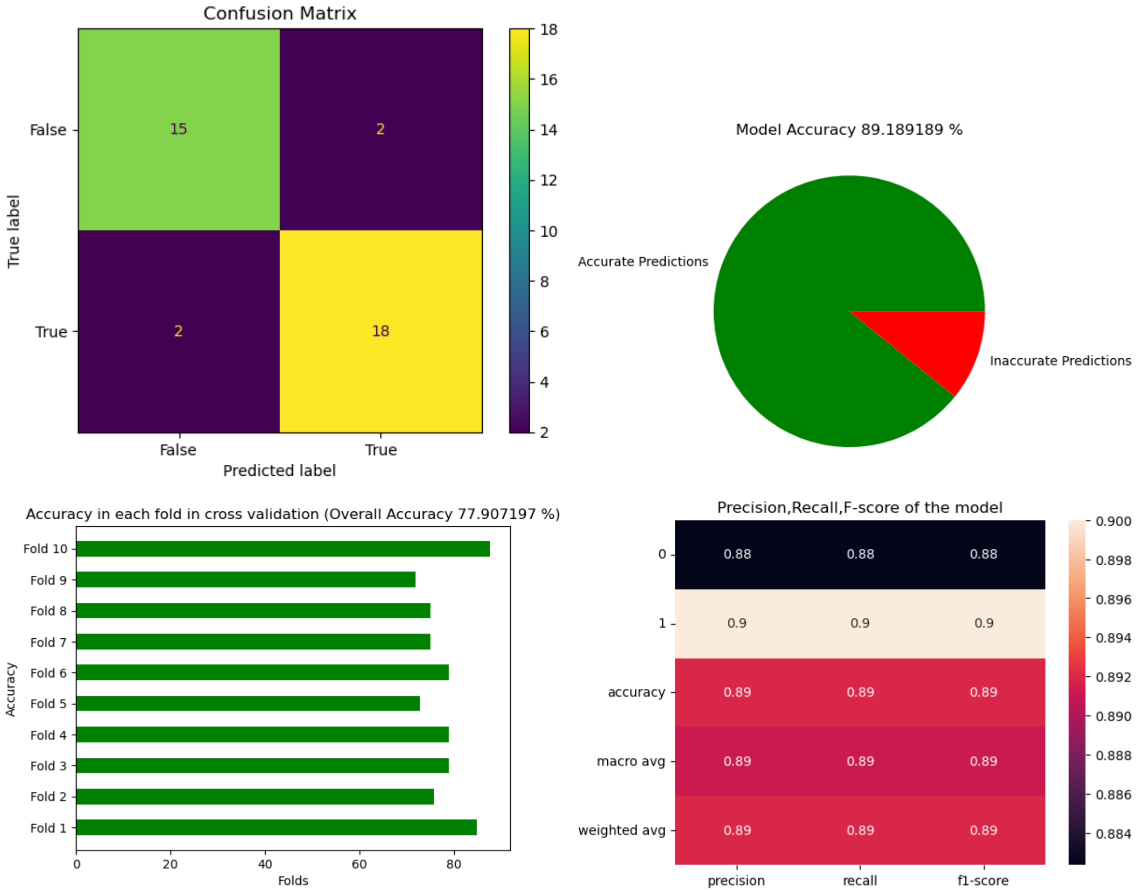


Figure 5.3: Different Performance Measures of COLUMBIA(colored) dataset

5.3 Discussion

The data and discussion in section 5.2 show that system performance varies depending on different factors such as block size and RBF kernel parameters (gamma, C). It depends on the system design and also the specific dataset what should be the appropriate values for these parameters. So to find the best combination of values for these parameters experimenting and tuning is the most practical and suitable way.

According to our test, the model's performance suffers when the block size is less than or more than 16x16. Therefore, we have decided to divide the photos into 16x16 blocks in order to train our system. Additionally, the experiment demonstrates that system performance suffers when gamma and C are set below or above the intended levels. The decision boundary of the SVM is influenced by the gamma value. Smaller values produce loose decision boundaries, which underfit the model. A higher gamma value causes the decision boundary to overfit the model. Our experiment reflects these occurrences as well.

Chapter 6

Conclusion

6.1 Conclusion

In our project, we have applied SVM along with DCT to classify authentic and tampered images. Currently, people are taking billions of pictures every day which have uses in many situations. But in some situations, the authenticity of these images becomes a matter of concern due to many reasons. The availability of many image editing tools makes these situations harder as nowadays anyone can tamper an image not needing any serious level of skills. In our project, we have built a system that can recognize tampered images using Copy move and Splicing techniques. Our system can recognize these types of image tampering with reliable accuracy and a reasonable amount of time.

6.2 Future Work

Future problems and scope changes for this project are expected to be many. The identification of these forgeries is also becoming a significant difficulty as forgery types of pictures change and progress. We'll improve the speed and accuracy with which our system can identify various intricate forms of picture counterfeiting, including filter-based forgery, retouching forgery, object removal forgery, and geometric forgery.

References

[1] Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, and Hassan Mathkour. Passive detection of image forgery using dct and local binary pattern. *International Journal of Advanced Computer Science and Applications*, 9(2):37–43, 2018.

[2] A. Parnak, Y. Baleghi Damavandi, and S. J. Kazemitabar. A novel image splicing detection algorithm based on generalized and traditional benford's law. *International Journal of Computer Science and Network Security*, 20(5):154–160, 2020.

[3] Mohammad Manzurul Islam, Gour Karmakar, Joarder Kamruzzaman, and Manzur Murshed. A robust forgery detection method for copy–move and splicing attacks in images. *Journal of Forensic Sciences*, 62(4):1036–1044, 2017.

[4] Shilpa Duaa, Jyotsna Singha, and Harish Parthasarathya. Image forgery detection based on statistical features of block dct coefficients. *Multimedia Tools and Applications*, 75(8):4495–4515, 2016.

[5] Toqeer Mahmood, Tabassam Nawaz, Rehan Ashraf, Mohsin Shah, Zakir Khan, Aun Irtaza, and Zahid Mehmood. A survey on block based copy move image forgery detection techniques. *Journal of King Saud University-Computer and Information Sciences*, 32(3):324–335, 2020.

[6] Soumen K. Patra and Abhijit D. Bijwe. Copy-move image forgery detection using svd. *International Journal of Computer Applications*, 117(20):33–38, 2015.

[7] Mohammed Hazim Alkawaz, Ghazali Sulong, Tanzila Saba, and Amjad Rehman. Detection of copy-move image forgery based on discrete cosine transform. *Journal of Visual Communication and Image Representation*, 52:118–128, 2018.

[8] Youtube. `https://www.youtube.com/watch?v=F5pMHaofd7c`. Accessed: May 2, 2023.

[9] Timo Ojala, Matti Pietikäinen, and Topi Mäenpää. Multiresolution grayscale and rotation invariant texture classification with local binary patterns. *Proceedings of the IEEE International Conference on Pattern Recognition*, 1:II–210–II–213, 2002.

[10] pyimagesearch. `https://pyimagesearch.com/2015/12/07/local-binary-patterns-with-python-opencv/`. Accessed: May 2, 2023.

[11] Javatpoint. `https://www.javatpoint.com/machine-learning-support-vector-machine-algorithm`. Accessed: May 2, 2023.