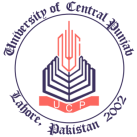
Copy Move Forgery Detection by Efficient Key-Point Based Method using Hybrid Feature Extraction



#### MASTER OF SCIENCE

#### IN

#### COMPUTER SCIENCE

Submitted By

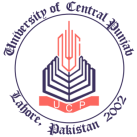
Hamad Malik

L1F19MSCS0020

#### DEPARTMENT OF COMPUTER SCIENCE FACULTY OF INFORMATION TECHNOLOGY

UNIVERSITY OF CENTRAL PUNJAB

Copy Move Forgery Detection by Efficient Key-Point Based Method using Hybrid Feature Extraction



A Thesis submitted in partial fulfillment

of the requirements for the degree of

#### MASTER OF SCIENCE

#### IN

#### COMPUTER SCIENCE

Submitted By

Hamad Malik

L1F19MSCS0020

Supervised By

Dr. Amjad Iqbal

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF INFORMATION TECHNOLOGY

UNIVERSITY OF CENTRAL PUNJAB

# ABSTRACT

The strategy being described in this study offers a complete approach to the detection of image fraud, utilizing a combination of unsupervised and supervised learning approaches. The unsupervised aspect of the process focuses on identifying latent patterns and structures within image datasets without relying on explicit labelling. This methodology is predicated upon the algorithm's inherent capacity to perceive and comprehend complex interconnections among data points, characteristics, and properties. The detection of image tampering heavily relies on several important unsupervised tasks, namely clustering, dimensionality reduction, density estimation, anomaly detection, and generative modeling. Various algorithms such as SURF, SIFT, Agglomerative Clustering, and RANSAC have been developed to provide effective solutions for this purpose. Simultaneously, the supervised technique leverages the potential of annotated datasets, facilitating the algorithm to provide informed predictions by considering input features. The described workflow involves several important stages, including thorough dataset preparation, the development of convolutional neural networks (CNNs), the training and evaluation of these networks, and the iterative refining process. The hyperparameters are meticulously tuned, and the Adam optimizer is utilized to reduce the Binary Cross-Entropy loss during the training procedure. The assessment of this technique entails a thorough evaluation of the performance of the model by employing several metrics such as precision, recall, F1 score, and accuracy. This evaluation is conducted on a specific validation dataset. Furthermore. In parallel, confusion matrices offer comprehensive insights into the performance of classification tasks. By combining the advantages of unsupervised techniques for feature extraction with the capabilities of supervised convolutional neural networks (CNNs) for image classification, this hybrid methodology aims to provide a resilient and precise solution for detecting image forgery. It ensures the accurate identification of manipulated images with a high level of precision and reliability.

# DEDICATION

To my parents, siblings, friends, supervisor and teachers, whose proficient guidance and splendid inspiration had positively influenced my life and made me capable of obtaining this degree successfully. They encouraged me to give it my full focus and effort. I could not have done this without them.

# ACKNOWLEDGEMENTS

I would like to acknowledge the efforts of all those people who have been involved one way or the other in completion of this thesis.

First of all, I am very much grateful to **ALMIGHTY ALLAH (SWT)** for giving me the opportunity and courage to complete this thesis successfully and helping me in each and every step of the way. I would like to thank my family for having faith in me and providing me with all the support and good wishes and for always taking my side whenever I needed them the most.

I am also thankful to my supportive and helpful supervisor **Dr. Amjad Iqbal** who guided and encouraged me in carrying out this research work and everything that I needed to know about research work throughout the thesis. His sage advice, insightful criticism, and patient encouragement aided the writing of this document in innumerable ways. His steadfast support of this thesis work was greatly needed and deeply appreciated.

# DECLARATION

I, Hamad Malik, S/O / D/O Mumtaz Ali, a student of “Degree Name” (e.g. MS/M.Phil. Business Administration), at “Faculty Name” (e.g. Faculty of Management Studies), University of Central Punjab, hereby declare that this thesis titled, “Title of Thesis” is my own research work and has not been submitted, published, or printed elsewhere in Pakistan or abroad. Additionally, I will not use this thesis for obtaining any degree other than the one stated above.

I fully understand that if my statement is found to be incorrect at any stage, including after the award of the degree, the University has the right to revoke my MS/M.Phil. degree.

Signature of Student:

Name of Student:

Registration Number:

Date:

**PLAGIARISM UNDERTAKING**

I solemnly declare that the research work presented in this thesis titled, “Defending Facial Recognition Models Against Adversarial Attack” is solely my research work, and that the entire thesis has been completed by me, with no significant contribution from any other person or institution. Any small contribution, wherever taken, has been duly acknowledged.

I understand the zero-tolerance policy of the HEC and University of Central Punjab towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and that every material used from other sources has been properly acknowledged, cited, and referenced.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis, even after the award of MS/MPhil. Degree, the University reserves the right to revoke my degree, and that HEC and the University have the right to publish my name on the HEC/University website for submitting a plagiarized thesis.

Signature of Student:

Name of Student: Hamad Malik

# CERTIFICATE OF RESEARCH COMPLETION

It is certified that this thesis titled, “Copy Move Forgery Detection by Efficient Key-Point Based Method using Hybrid Feature Extraction”, submitted by Hamad Malik, Registration No. L1F19MSCS0020, for MS. Degree at “Faculty of Information Technology”, University of Central Punjab, is an original research work and contains satisfactory material to be eligible for evaluation by the Examiner(s) for the award of the above stated degree.

##### Dr. Amjad Iqbal

Dean FOIT

Faculty: Faculty of Information Technology University of Central Punjab

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# CERTIFICATE OF EXAMINERS

It is certiﬁed that the research work contained in this thesis titled “Introducing Approach to make the CBIR Fusion technique scale-invariant and noise-rebust” is up to the mark for the award of “Master of Science in Computer Science”.

**Internal Examiner External Examiner**

Signature: Signature:

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Dean

Faculty of Information Technology

University of Central Punjab

Signature:

Name:

Date:

# TABLE OF CONTENTS

Contents

[ABSTRACT 3](#_Toc152432622)

[DEDICATION 4](#_Toc152432623)

[ACKNOWLEDGEMENTS 5](#_Toc152432624)

[DECLARATION 6](#_Toc152432625)

[CERTIFICATE OF RESEARCH COMPLETION 8](#_Toc152432626)

[CERTIFICATE OF EXAMINERS 9](#_Toc152432627)

[TABLE OF CONTENTS 10](#_Toc152432628)

[LIST OF FIGURES 12](#_Toc152432629)

[CHAPTER ONE: INTRODUCTION 14](#_Toc152432630)

[1.0 Supervised vs unsupervised learning 17](#_Toc152432631)

[1.1 Types of forgery 21](#_Toc152432632)

[1.2 Background of Problem 22](#_Toc152432633)

[1.3 Research Gap 28](#_Toc152432634)

[1.4 Problem Statement 31](#_Toc152432635)

[1.5 Aims and Objective 32](#_Toc152432636)

[1.6 Summary 33](#_Toc152432637)

[CHAPTER TWO: LITERATURE REVIEW 35](#_Toc152432638)

[2. SIFT for object detection 36](#_Toc152432639)

[2.0 Superpixel for the landscape of forgery detection 38](#_Toc152432640)

[2.1 Helmert Transformation 39](#_Toc152432641)

[2.2 AKAZE for the extraction of descriptor 43](#_Toc152432642)

[2.3 RANSAC for key point distinguish between original and fake image 45](#_Toc152432643)

[CHAPTER THREE: RESEARCH METHODOLOGY 47](#_Toc152432644)

[3. Dataset Search 47](#_Toc152432645)

[3.0 Implemented Technique 50](#_Toc152432646)

[3.1 Architectural Diagram 51](#_Toc152432647)

[3.2 Unsupervised Approach 52](#_Toc152432648)

[*3.2.1* *Surf* 54](#_Toc152432649)

[*3.2.2* *SIFT* 55](#_Toc152432650)

[*3.2.3* *Aglometric clustering* 57](#_Toc152432651)

[*3.2.4* *Ransac* 59](#_Toc152432652)

[3.3 Supervised Approach 61](#_Toc152432653)

[*3.3.1* *Dataset Prepration* 63](#_Toc152432654)

[*3.3.2* *CNN* 64](#_Toc152432655)

[*3.3.3* *Flatten and fully connected layers* 66](#_Toc152432656)

[*3.3.4* *Output layer* 67](#_Toc152432657)

[*3.3.5* *Hyperparameter Setting* 68](#_Toc152432658)

[*3.3.6* *Optimizer* 68](#_Toc152432659)

[*3.3.7* *Accuracy of the model* 69](#_Toc152432660)

[CHAPTER FOUR: FINDINGS (Or RESULTS) 70](#_Toc152432661)

[4. Configuration Settings 70](#_Toc152432662)

[4.0 Results of these applied techniques 70](#_Toc152432663)

[*4.0.1* *Unsupervised Approach results* 70](#_Toc152432664)

[*4.0.1.1* *Surf* 70](#_Toc152432665)

[*4.0.1.2* *SIFT* 71](#_Toc152432666)

[*4.0.1.3* *Aglometric Clustering* 72](#_Toc152432667)

[*4.0.1.4* *RANSAC* 72](#_Toc152432668)

[4.0.2 Supervised Learning approach Results 74](#_Toc152432669)

[*4.0.2.1* *Graph Validation loss* 74](#_Toc152432670)

[*4.0.2.2* *Graphs for Accuracy* 74](#_Toc152432671)

[*4.0.2.3* *Graphs for Precision* 75](#_Toc152432672)

[*4.0.2.4* *Graphs for Recall* 76](#_Toc152432673)

[*4.0.2.5* *Graphs for F1score* 77](#_Toc152432674)

[*4.0.2.6* *Graphs for ROC* 77](#_Toc152432675)

[*4.0.2.7* *Confusion matrix* 79](#_Toc152432676)

[4.0.3 Results comparison between different techniques 80](#_Toc152432677)

[CHAPTER FIVE: DISCUSSION 81](#_Toc152432678)

[CHAPTER SIX: CONCLUSION AND FUTURE WORK 83](#_Toc152432679)

[REFERENCES 85](#_Toc152432680)

# LIST OF FIGURES

[Figure 1- SURF Accuracy 68](#_Toc146508654)

[Figure 2- SIFT Accuracy 68](#_Toc146508655)

[Figure 3Aglometric Clustering Accuracy 69](#_Toc146508656)

[Figure 4- Accuracy of RANSAC 70](#_Toc146508657)

[Figure 5- Applying all the above unsupervised algorithms 70](#_Toc146508658)

[Figure 6- Graph of validation 71](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508659)

[Figure 7- Graph od Accuracy 71](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508660)

[Figure 8- Graph of precision 72](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508661)

[Figure 9- Graph of Recall 72](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508662)

[Figure 10- Graph of F1 Score 73](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508663)

[Figure 11- Graph for ROC 73](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508664)

[Figure 12- Confusion Matric 74](file:///C:\Users\DELL\Desktop\Hamad%20Malik%20thesis.docx#_Toc146508665)

**LIST OF ABBREVIATIONS AND ACRONYMS**

**CMF** Copy Move Forgery

**CNN** Convolutional Neural Network

**RANSAC** Random Sample Consensus

**SIFT** Scale-Invariant Feature Transform

**SURF** Speeded-Up Robust Features

# CHAPTER ONE: INTRODUCTION

In the present day, we find ourselves deeply entrenched in an exceptionally astonishing epoch of technological advancements. In contemporary society, there exists a pervasive integration of the digital domain into various aspects of human life, encompassing both individual inclinations and professional practises. The proliferation of technology in its diverse manifestations has emerged as the predominant catalyst shaping our contemporary societal framework.

The Internet, specifically, emerges as the epitome of our everyday lives. The pervasive integration of technology in our daily lives has resulted in a seamless connection to individuals and serves as a portal to the ever-changing global environment. The utilisation of this vast digital network enables individuals to maintain connections with their social circles and stay continually updated on global events. The Internet has emerged as a crucial instrument for facilitating communication, facilitating the acquisition of knowledge, and ensuring individuals remain informed about the latest developments and notable events.

One notable facet of modern society is to the extensive utilisation of social media platforms. The aforementioned platforms, namely Facebook, Instagram, and Twitter, have solidified their position as integral components of contemporary modes of communication. Every day, a vast number of individuals actively participate in these digital platforms, employing them as mediums for self-expression and fostering social interactions. One of the most prominent characteristics of social media is the extensive quantity of digital photographs and movies that are exchanged among members. Essentially, it has evolved into a virtual exhibition space where individuals exhibit their personal lives, disseminate their distinctive experiences, and chronicle their thrilling escapades. In the contemporary era of digital communication, images and videos have emerged as a widely adopted medium for effectively expressing emotions, recounting personal experiences, and narrating stories.

Nevertheless, in addition to personal expression and social interaction, multimedia, namely images, assumes an increasingly crucial function in diverse key sectors. In the context of a legal proceeding, such as a courtroom setting, visual representations have evolved as highly effective instruments for the presentation of evidence. They are utilised to strengthen legal assertions and offer visual evidence in both criminal and civil litigation. The utilisation of visual representations as corroborative proof in criminal cases has emerged as a pivotal component of contemporary investigative practises, significantly assisting law enforcement entities in their endeavours to uphold the principles of fairness and equity within the legal system.

Furthermore, the practical implementation of specialised object tracking and area detection has been observed in various domains, including security and surveillance. These applications enable the real-time monitoring of items and places of interest. Within the field of programmetry, which involves the measurement of objects and distances using photographs, developments in technology have resulted in the development of more precise and efficient procedures. These advancements have facilitated accurate measurements and analysis for a wide range of applications, including but not limited to construction and archaeology.

In conclusion, we currently reside in a highly sophisticated era characterised by significant technical advancements, wherein the Internet and social media play a crucial role in our day-to-day existence. The dissemination of multimedia content, particularly visual images and videos, has become an omnipresent mode of communication and self-representation. Concurrently, photos have surpassed their initial purpose for personal utilisation and have become indispensable instruments in several domains, including but not limited to the legal system, scientific research, and data analysis. The ever-evolving nature of technology and multimedia has had a tremendous influence on our lives, with the promise of even more astonishing advancements in the future. As we traverse this dynamic environment, it becomes apparent that our dependence on technology and multimedia will continue to intensify, exerting a significant influence on the trajectory of human development throughout this pivotal period characterised by technical advancements.

The internet has emerged as an indispensable component of contemporary society, revolutionising modes of communication, facilitating information retrieval, and enabling manipulation of digital content. The proliferation of online technologies in the contemporary digital era has significantly transformed the manner in which individuals engage with visual content. These software applications provide consumers with the ability to easily edit, enhance, or change photos, giving a range of capabilities such as object removal, text addition, and various other modifications. Nevertheless, as we explore the domain of digital alteration, inquiries regarding the genuineness and legitimacy of photographs emerge as prominent issues, giving rise to substantial apprehensions over their societal implications.

Adobe Photoshop, in addition to a wide array of other robust online editing tools, has significantly contributed to this transformative process. These software applications include interfaces that are designed to be easily navigable by users with less technical proficiency, enabling them to effortlessly make modifications to photographs. Although the primary purpose of these tools was originally to augment creativity and digital artwork, they have also evolved into platforms for engaging in mischievous and deceptive activities.

In the context of social media, it is common for individuals to engage in picture alteration as a means of portraying an idealised representation of oneself. This practise perpetuates unattainable beauty ideals and consequently contributes to the development of diminished self-esteem among its users. Furthermore, the utilisation of modified photographs can be strategically employed as a means of disseminating propaganda, thereby instigating a sense of scepticism and disharmony within the general public. Within the realm of journalism, the proliferation of fabricated news stories and manipulated visual content has significantly undermined the public's confidence in the media, hence presenting a formidable obstacle in the discernment of veracity from falsehood.

Furthermore, the ramifications of picture modification encompass both legal and ethical considerations. The utilisation of modified photos as evidence within courtrooms gives rise to inquiries regarding their legitimacy and dependability. This presents a significant obstacle to the legal system and the quest for veracity. Here are the some of the forgery techniques.

Supervised vs unsupervised learning

### Supervised vs unsupervised learning

**Supervised Learning:**

In supervised learning, algorithms are trained on labeled datasets, where each input is paired with a corresponding output. The essence of this paradigm lies in learning a mapping from inputs to outputs based on the provided labeled examples. The primary goal is to equip the algorithm with the ability to make accurate predictions or classifications for new, unseen data points by leveraging the learned patterns from the training data. Supervised learning encompasses tasks such as classification, where the algorithm assigns data points to predefined categories, and regression, where it predicts continuous values. This paradigm is particularly well-suited for scenarios where the desired outcome or target variable is known and can be explicitly provided during training. The effectiveness of supervised learning relies on the quality and representativeness of the labeled data, and it finds widespread application in various domains, including image recognition, natural language processing, and medical diagnosis.

**Supervised Learning Techniques:**

Supervised learning encompasses various techniques designed for scenarios where the algorithm is provided with labeled training data, allowing it to learn patterns and relationships between inputs and corresponding outputs.

1. **Linear Regression:** Linear regression is employed for predicting a continuous outcome variable based on one or more predictor variables. For instance, it could predict house prices using features like square footage and number of bedrooms.
2. **Logistic Regression:** Logistic regression is used for binary or multiclass classification problems. It could be applied, for instance, to classify emails as spam or non-spam.
3. **Decision Trees:** Decision trees are tree-like models used for both classification and regression tasks. They could predict customer purchases based on various demographic factors.
4. **Support Vector Machines (SVM):** SVM is effective for classification tasks, aiming to find a hyperplane that best separates different classes. It could be used for image classification tasks like recognizing handwritten digits.
5. **Random Forest:** Random Forest is an ensemble learning method utilizing multiple decision trees for improved accuracy and robustness. It might be employed to predict customer churn in a subscription-based service.
6. **Neural Networks:** Neural networks, especially deep learning models, consist of interconnected layers of nodes and are suitable for complex tasks. They are widely used, for example, in image recognition tasks using convolutional neural networks (CNNs).

**Unsupervised Learning:**

In contrast, unsupervised learning operates in scenarios where the algorithm is presented with unlabeled data and tasked with discovering inherent patterns, structures, or relationships without explicit guidance on the correct output. Unsupervised learning tasks include clustering, where the algorithm groups similar data points together, dimensionality reduction to simplify complex datasets, density estimation for understanding data distributions, anomaly detection to identify unusual patterns, and generative modeling to create new data samples resembling the training set. Unsupervised learning is particularly valuable when the nature of the underlying data is not well understood, and the goal is to explore and reveal hidden structures. This paradigm enables the algorithm to autonomously extract meaningful information from unstructured or unlabelled datasets, making it a crucial tool for data exploration and gaining insights into the intrinsic characteristics of the data.

**Unsupervised Learning Techniques:**

Unsupervised learning involves techniques where the algorithm is presented with unlabeled data and tasked with discovering inherent patterns, structures, or relationships without explicit guidance.

1. **K-Means Clustering:** K-Means clustering divides data points into k clusters based on similarity. This technique is commonly used for customer segmentation in marketing.
2. **Hierarchical Clustering:** Hierarchical clustering organizes data points into a tree-like hierarchy, representing relationships between clusters. It could be applied, for example, in creating taxonomies based on biological species similarities.
3. **Principal Component Analysis (PCA):** PCA reduces dimensionality by transforming data into a new coordinate system. It finds application in tasks such as compressing images while retaining essential features.
4. **t-Distributed Stochastic Neighbor Embedding (t-SNE):** t-SNE is used to reduce dimensionality while preserving pairwise similarities between data points. It is often employed for visualizing high-dimensional data in two or three dimensions.
5. **Density-Based Spatial Clustering of Applications with Noise (DBSCAN):** DBSCAN identifies clusters based on density differences in the data. This technique is useful, for example, in identifying outliers or anomalies in network traffic.
6. **Generative Adversarial Networks (GANs):** GANs are a type of generative model where two neural networks compete to generate realistic data. They find application in generating realistic images that resemble a given dataset.

**Why the adversarial are not the part of system before**

Adversarial attacks are closely associated with supervised learning due to several key factors. Firstly, these attacks often exploit gradient information to iteratively modify input data in a manner that maximizes the model's loss. In supervised learning scenarios, where a clear objective function, such as cross-entropy loss, guides the model's training, this gradient information is readily available. Moreover, adversarial attacks in supervised settings frequently take the form of targeted attacks, involving the crafting of perturbations to deliberately force the model to misclassify an input as a specific incorrect class. This targeted nature aligns closely with the overarching goal of influencing model predictions in the context of supervised learning tasks. Additionally, the vulnerability of models in supervised learning to adversarial perturbations is heightened by their training process, where models are explicitly trained to minimize a specific objective function based on labeled data. This susceptibility makes them more prone to manipulations that exploit and alter this objective. However, it's important to note that ongoing research is exploring adversarial attacks and defenses in unsupervised learning scenarios. Efforts in adversarial training techniques and methods to enhance the robustness of unsupervised models reflect active investigations within the machine learning community.

### Types of forgery

**Splicing or Joining**: Splicing, or joining, is a forgery technique where multiple images are combined to create a composite image. This can include merging different photographs or altering the context of a scene. Detecting splicing involves analyzing variations in lighting, color tones, and other subtle differences between the spliced elements. Advanced image forensics may employ techniques such as shadow analysis or inconsistency in noise patterns to identify spliced regions.

**Retouching and Airbrushing:** Retouching and airbrushing involve digitally altering specific features of an image to enhance its visual appeal. This may include removing imperfections, adjusting skin tone, or modifying physical attributes. Detecting such forgery often requires comparing the manipulated image with the original to identify unnatural alterations in texture, color consistency, or the overall visual coherence of the image.

**Object Removal:** Object removal forgery entails erasing elements or individuals from an image to alter its narrative or context. Forensic analysis in such cases focuses on identifying inconsistencies in the background, shadows, and lighting where the object was removed. This can involve examining pixel-level details and changes in the image structure.

**Color Manipulation:** Color manipulation forgery involves altering the colors in an image to convey a different mood or message. Detecting this type of forgery may involve analyzing color histograms and checking for unnatural shifts in color tones. Additionally, forensic experts may look for inconsistencies in lighting conditions and shadows that could indicate digital manipulation.

**Forgery through Filters and Effects:** Forgery through filters and effects entails applying various digital filters or effects to an image to distort its appearance. Detection involves recognizing the specific artifacts left by these filters, such as unusual patterns, noise, or color aberrations. Analyzing the metadata of the image and comparing it with the expected results of certain filters can also aid in identifying this type of forgery.

**Deepfake Technology:** Deepfake technology involves using advanced machine learning algorithms to create highly realistic fake images or videos. This includes swapping faces, mimicking voices, or generating entirely fabricated content. Detecting deepfakes requires sophisticated analysis, including facial feature recognition, lip-syncing scrutiny, and assessing the consistency of facial expressions and lighting throughout the video.

**Text and Graphic Overlay:** Text and graphic overlay forgery involves adding or altering textual and graphic elements on an image to change its meaning or convey false information. Forensic analysis typically focuses on examining the consistency of fonts, text alignment, and graphic elements within the image. Additionally, experts may investigate the metadata and layer information to identify any added elements that might not align with the original composition.

### Background of Problem

In summary, the widespread availability of free internet image altering tools has initiated a period in which the veracity of visual output is consistently subject to scrutiny. While these The study described in thesis [14] aims to significantly transform the field of copy-move forgery detection in a single image by utilising the advanced AKAZE (Accelerated-KAZE) features. The primary objective is to improve the accuracy, dependability, and adaptability in identifying modified areas that closely resemble authentic information.

The extraction of descriptors is a crucial step in this unique approach, which is helped by the Modified Local Binary Pattern (LBP) technique. The descriptors utilised in this study were obtained by methodically extracting key-points from the target image using the AKAZE algorithm. The selection of AKAZE as the foundation of this methodology is motivated by its inherent capability to effectively handle intricate changes and variations in images, rendering it highly suitable for the purpose of detecting forgeries.

In order to differentiate authentic content from possible forgeries, the study utilises the Random Sample Consensus (RANSAC) method. The algorithm exhibits a high level of intelligence as it effectively analyses the main points, accurately differentiating between genuine components and incorrect associations. Through the process of eliminating false positives, the system is able to refine its precision and enhance its ability to withstand different types of image alteration.

In the context of thorough experimental evaluations, this methodology demonstrates considerable potential. This technology demonstrates superior performance compared to previous and concurrent methods in addressing a variety of obstacles, such as image rotation, blurring, the presence of noise, and the well-known vulnerabilities associated with JPEG compression attacks. Significantly, the system's exceptional ability to detect instances of "Object Removal with uniform Background forgery" is a noteworthy accomplishment, surpassing alternative approaches and setting a higher standard for precision and dependability.

Nevertheless, the genuine originality of this study resides not alone in its concrete outcomes, but also in its forward-thinking methodology towards the field of digital forensics. The aforementioned concept presents a novel paradigm that surpasses the primary objective of identifying forgeries and goes into the broader framework of resilience in digital systems.

This approach advocates for the belief that the consideration of robustness should not be an incidental consideration but rather an essential aspect of every digital system. The presented approach offers a comprehensive perspective on the detection of image forgery, aiming to achieve accuracy while also simplifying system complexity and minimising computational burden. Essentially, it promotes the idea of a comprehensive solution that surpasses the limitations of forgery detection and extends throughout the entirety of the digital ecosystem.

Significantly, it directly addresses the complex issues presented by digital forgeries. The matters pertaining to the robustness of the system, the resilience of detection in smooth, symmetrical, and recurrent areas, and the capability to identify forgeries in non-affine transformation zones are thoroughly examined with great enthusiasm and resolve.

Within the ever-evolving realm of digital forensics, this study signifies a significant achievement, a critical juncture where accuracy and resilience intersect to mould the trajectory of counterfeit identification. In the current period, marked by a growing dependence on digital media, notable initiatives are being undertaken to establish a secure and reliable digital environment. These endeavours aim to safeguard the authenticity and reliability of the content that shapes our networked existence. The study described in thesis [14] aims to significantly transform the field of copy-move forgery detection in a single image by utilising the advanced AKAZE (Accelerated-KAZE) features. The primary objective is to improve the accuracy, dependability, and adaptability in identifying modified areas that closely resemble authentic information.

At the core of this novel methodology lies the extraction of descriptors, a crucial process enabled by the Modified Local Binary Pattern (LBP) technology. The descriptors utilised in this study are obtained through the painstaking extraction of key-points using the AKAZE algorithm from the target image. The selection of AKAZE as the fundamental element of this methodology is motivated by its inherent capability to effectively handle intricate changes and variations in images, rendering it highly suitable for the purpose of detecting forgeries.

In order to differentiate authentic content from possible forgeries, the study utilises the Random Sample Consensus (RANSAC) method. The clever algorithm exhibits a high level of accuracy in its ability to analyse and differentiate between original elements and false matches, effectively dissecting the key-points. Through the process of eliminating false positives, the system undergoes fine-tuning to enhance its precision and strengthen its ability to withstand different types of image alteration.

In the context of thorough experimental evaluations, this methodology demonstrates considerable potential. This technology demonstrates superior performance compared to previous and concurrent methods in addressing a wide range of obstacles, such as image rotation, blurring, the presence of noise, and the well-known vulnerabilities associated with JPEG compression attacks. Significantly, the system's exceptional ability to detect instances of "Object Removal with uniform Background forgery" is a noteworthy accomplishment, surpassing alternative approaches and setting a higher standard for precision and dependability.

Nevertheless, the genuine uniqueness of this study is not alone in its concrete outcomes, but more in its visionary perspective towards the field of digital forensics. This paradigm presents a novel framework that goes beyond the primary objective of detecting forgery and explores the broader structure of resilience in digital systems.

This approach advocates for the belief that the concept of robustness should not be considered as an insignificant consideration, but rather as an essential aspect of every digital system. The presented approach offers a comprehensive perspective on the detection of image forgery, aiming to achieve accuracy while also simplifying system intricacies and minimising computational burden. Essentially, it promotes the adoption of a holistic solution that surpasses the confines of forgery detection and extends throughout the entirety of the digital ecosystem.

Significantly, it directly addresses the complex issues presented by digital forgeries. The matters pertaining to the robustness of the system, the resilience of detection in regions that are smooth, symmetrical, and recurrent, and the capability to identify forgeries in regions with non-affine transformations are all thoroughly examined with great enthusiasm and resolve.

Within the ever-evolving realm of digital forensics, this study signifies a significant achievement, a critical juncture where accuracy and resilience intersect to mould the trajectory of counterfeit detection in the next years. In the current period, marked by a growing dependence on digital media, notable initiatives are being undertaken to establish a secure and reliable digital environment. These endeavours aim to safeguard the authenticity and reliability of the content that shapes our networked existence.

While tools present opportunities for creativity, they also possess the capacity to destabilise established cultural norms, propagate misinformation, and erode faith in diverse institutions. In the context of our evolving digital environment, it is imperative to achieve a harmonious equilibrium between artistic ingenuity and conscientious utilisation. Simultaneously, it is crucial to cultivate the capacity for discernment, enabling the differentiation between authentic and manipulated visual content within our progressively interconnected global society.

The significance of digital photographs is progressively increasing in our daily lives as society advances. Digital photographs serve as a means of communication and encompass a substantial amount of significant information. For example, a dependable digital image can serve as admissible evidence within a court of law. Additionally, daily newspapers and magazines have a strong association with digital photographs. Furthermore, medical professionals commonly employ digital photos to aid in the diagnosis of various ailments. Nevertheless, the prevalence of high-end digital cameras and photo-editing programmes is increasing. Consequently, the process of manipulating digital photographs has become considerably uncomplicated, enabling the creation of counterfeit images that pose challenges in discerning their authenticity from genuine photographs. The realism and integrality of digital visuals are currently facing significant challenges. Therefore, acquiring the skill is imperative and essential in discerning authentic images from counterfeit ones. The field of digital picture forensics technology is quite nascent, as one would anticipate given the circumstances. The body of evidence is comprised of active components. The presence of evidence is contingent upon whether the additional data is passive-blind, and digital photos possess either embedded information or lack thereof. The scope of active methods is restricted by this prerequisite. Two examples of these strategies include watermarking and utilising the camera's digital signature. Non-intrusive/blind methodologies, also known as passive techniques, do not require any data to be embedded into the digital image. The manipulation of digital images can be achieved by several techniques, including but not limited to rotation, scaling, resizing, noise addition, blurring, and compression, so enabling the creation of counterfeit visual representations.

In the era of digital technology, the capabilities of image manipulation techniques have advanced significantly, allowing humans to manipulate visual content in a multitude of intricate ways. Within the realm of forging techniques, two notable types emerge as particularly prominent: Copy-Move forging and Splicing Forgery. Although these methods differ in their implementation, they all aim to modify photographs while preserving a sense of authenticity. This extensive investigation examines the complexities associated with various forms of forgeries, the difficulties they present, and the growing strategies utilised to identify and counteract them.

### Research Gap

Copy-Move Forgery represents a passive form of manipulation, where a specific region of an original image is copied and pasted within the same image. This technique is often employed to either replicate or obscure objects within the frame, creating the illusion of multiple identical elements. Detecting Copy-Move Forgery is an arduous task because perpetrators meticulously manipulate the duplicated region to seamlessly blend with the surrounding content. To achieve this, various post-processing operations such as rescaling, affine transformations, resizing, and blurring are applied to the copied area. These adjustments make it exceedingly challenging for conventional forensic tools to identify the tampering.

Copy-move forgery can be categorized into several types based on the nature and complexity of the manipulation involved. The main types of copy-move forgery include:

1. Direct Copy-Move Forgery: In this basic form of copy-move forgery, a portion of the image is directly copied and pasted to another location within the same image. The copied portion is often identical or nearly identical to the original.
2. Scaled Copy-Move Forgery: In this variation, the copied portion may be resized (scaled) before it is pasted into another part of the image. Resizing can involve both enlarging and shrinking the copied region to make it appear as if it belongs naturally in the new location.
3. Rotated Copy-Move Forgery: Here, the copied region is rotated to a different angle before being pasted elsewhere in the image. This adds complexity to the forgery and makes it harder to detect.
4. Blended Copy-Move Forgery: In blended copy-move forgery, the copied region is not only pasted but also blended seamlessly into the surrounding pixels to make the manipulation less obvious. This may involve adjusting colors, brightness, and contrast.
5. Multiple Copy-Move Forgery: In some cases, forgers may perform multiple copy-move operations within the same image, creating a more intricate deception by duplicating or relocating several objects or regions.
6. Non-Contiguous Copy-Move Forgery: While traditional copy-move forgery involves contiguous regions, non-contiguous copy-move forgery may involve copying and pasting multiple non-adjacent regions from one part of the image to another, making detection even more challenging.
7. Cross-Format Copy-Move Forgery: This type involves copying an element from one image and pasting it into another image, often with different formats or resolutions. It can be used to create more complex and sophisticated forgeries.

Detecting these various types of copy-move forgery typically requires advanced image processing and forensic techniques, as well as the use of specialized software tools and algorithms designed to identify duplicated or manipulated regions within digital imagesTop of Form

In contrast, Splicing Forgery involves integrating a substantial portion of an external image into the original one. This method allows for the addition or replacement of objects in a manner that can be more convincing than Copy-Move Forgery. To ensure a seamless integration, the spliced region undergoes a series of transformations before being pasted into the target image. These transformations may include resizing, flipping, and blurring, among others, making it even more difficult for forensic analysts to detect the tampering.

It is worth emphasizing that merely copying and pasting elements from one image to another is insufficient to create convincing forgeries. Perpetrators employ a plethora of advanced techniques to manipulate and conceal their alterations. They often leverage sophisticated image editing software to restore and resize the copied region, ensuring it aligns seamlessly with the target image. Additionally, strategic flipping and blurring may be applied to further obscure the manipulated area, rendering it increasingly challenging to detect the tampering.

The detection of image forgeries has become a pressing concern in various fields, including forensics, journalism, and law enforcement. Digital image forensics experts employ an array of tools and methodologies to unveil these manipulations. They meticulously analyze the image's metadata, scrutinize inconsistencies in lighting and shadows, and examine pixel-level details to identify discrepancies that may indicate tampering. In recent years, the integration of machine learning and artificial intelligence techniques has significantly enhanced the accuracy and efficiency of forgery detection.

However, despite the advancements in forgery detection methods, the field is far from being highly optimized. There remain numerous gaps and challenges that demand further discussion and research. One notable approach to addressing these issues is the key-point-based copy-move forgery detection method.

Key-point-based detection relies on the identification of distinctive points in the image, known as key points. These key points are determined using descriptors such as Scale-Invariant Feature Transform (SIFT). In the context of copy-move forgery detection, key points serve as markers for identifying regions that may have been manipulated. The motivation behind this approach is to enhance the accuracy of detection beyond the capabilities of existing methods.

A novel variation in achieving this goal involves the utilization of Key-Point Extraction in conjunction with Hybrid Feature Extraction methods and Hierarchical Clustering for Copy-Move Forgery Detection. By combining these techniques, the system gains robustness and becomes more adept at identifying tampered regions within an image. This innovative approach is driven by the pursuit of greater accuracy and precision in detecting and verifying the authenticity of images.

In conclusion, the realm of image manipulation and forgery detection is continually evolving as technology advances. Copy-Move Forgery and Splicing Forgery represent two prevalent methods used to alter images, each presenting its unique challenges to forensic analysts. While progress has been made in detecting these forgeries, there is still much ground to cover. Innovations in key-point-based detection, hybrid feature extraction, and hierarchical clustering techniques hold promise for further improving the accuracy and robustness of forgery detection systems. As we navigate this ever-changing landscape, it is crucial to stay at the forefront of research and development to ensure the integrity and authenticity of visual content in an increasingly digital world.

### Problem Statement

Robustness in copy-move forgery detection systems remains a key challenge in the digital landscape. While research has addressed this issue, achieving complete optimization is elusive, with models showing varying degrees of strength. Current systems reach a precision of 92.5%, indicating room for improvement. Notably, detecting modified images with smooth, symmetrical, and recurrent regions remains an underexplored area. While progress has been made in identifying tampering after affine transformations, challenges persist with non-affine transformations. The primary focus is on continual improvement and exploring adversarial training to enhance the resilience of these systems against hostile attacks. This pursuit is crucial for maintaining the integrity of digital content across diverse sectors.

### Aims and Objective

* + 1. The primary goal of this project is to increase the system's resilience, with the ultimate goal being the achievement of unmatched accuracy. This audacious endeavour is supported by the application of a cutting-edge method called hybrid feature extraction. This strategy aims to produce a synergistic impact by combining and utilising the advantages of various feature extraction techniques, raising the system's precision to previously unattainable levels. This new approach is a significant step towards improving the system's performance and aims to establish new standards for reliability and effectiveness.
    2. Building upon the groundwork established by earlier studies, the goal of this project is to develop cutting-edge methods and algorithms that surpass the work of their forebears in the field of forgery detection. The unique selling point is the careful selection and application of cutting-edge techniques that are carefully crafted to surpass earlier efforts. This involves a thorough investigation of state-of-the-art algorithms, each carefully chosen for its capacity to identify even the most complex and sophisticated types of forgeries, setting a higher bar for precision and efficacy in this vital area.
    3. Using the CASIA V2 dataset, a set of rigorous experiments will be carried out to assess the system's performance and validate the effectiveness of our proposed changes. This dataset acts as an essential testing ground, providing a wide range of real-world situations and difficulties for the system to face. Through the application of this benchmark dataset, we hope to thoroughly evaluate our system's capabilities and measure its overall performance in a range of scenarios. Because of its complexity and diversity, CASIA V2 is a suitable candidate for benchmarking, which allows us to determine the system's flexibility and efficacy in a wide range of forging scenarios. This guarantees the dependability and real-world relevance of our innovations in the field of forgery detection.

### Summary

In the contemporary era characterised by digital advancements, technology assumes a crucial position in our daily existence, exerting a profound impact on several domains, encompassing individual inclinations as well as professional practises. The internet serves as a global medium that facilitates connectivity, enabling individuals to engage in conversation, acquire knowledge, and remain updated on global affairs. Social media platforms such as Facebook, Instagram, and Twitter have become indispensable tools in contemporary communication, as they enable users to engage in self-expression through the universal language of photos and videos. In addition to their utility in personal contexts, photographs play a critical role across other areas. photographs have a crucial role as evidentiary material in court procedures, while several industries such as security, surveillance, and programmetry heavily depend on the meticulous examination of photographs. Nonetheless, the accessibility of picture alteration through software such as Adobe Photoshop gives rise to apprehensions regarding veracity, resulting in the emergence of problems such as unattainable ideals of physical attractiveness, dissemination of false information, and legal disputes within the judicial system. In order to effectively tackle these challenges, it is imperative to prioritise research in the field of picture forensics. This encompasses the identification of copy-move and splicing forgery techniques, wherein images undergo modifications while preserving their originality. The present state of forgery detection techniques is characterised by ongoing advancements; nonetheless, some obstacles persist. These challenges encompass the attainment of resilience, the detection of diverse forms of forgery, and the handling of non-affine changes. Promising advancements in accuracy and durability against adversarial attacks can be achieved by the utilisation of innovative techniques, such as key-point-based detection and hybrid feature extraction. The primary objective is to uphold the integrity and genuineness of digital photography within the context of an ever-expanding digital landscape.

# CHAPTER TWO: LITERATURE REVIEW

This section necessitates the inclusion of a comprehensive evaluation of recent scholarly literature that is pertinent to the research being conducted. It is imperative to acknowledge that the literature review should refrain from merely listing individual works, but rather should encompass a comprehensive analysis of the prevailing themes, connections, and potential inquiries or deficiencies that may emerge from the discourse. The inclusion of a mere compilation of many research is insufficient; instead, it is imperative to expound upon one's point inside this part, drawing upon pertinent literature.

Numerous diligent researchers have made efforts to expand the possibilities in the field of digital forensics, aiming to improve the accuracy and reliability of forgery detection systems. The collaborative endeavours of individuals have given rise to inventive solutions and tactics designed to enhance the robustness of these systems in the face of constantly changing methods of digital manipulation. An issue that has arisen in the current era of digital technology is the problematic phenomenon known as Copy-Move forgery. This deceptive method of altering images involves the deliberate placement of both genuine and fraudulent elements within a single frame, with the intention of misleading both human observers and automated detection systems.

The issue of copy-move forgery presents a significant obstacle since it involves creating a strong resemblance between the altered and authentic sections of an image. These regions demonstrate a complex interplay of related attributes, including similar patterns, subtle variations in shading, the inclusion of noise, and harmonious pairings of colours. As the level of expertise exhibited by forgers continues to increase, there arises a pressing necessity for the development of detection systems that are as advanced.

Scholars have made significant advancements in addressing this urgent matter, with two prevailing frameworks emerging as prominent: block-based and key-point-based detection strategies. The block-based methodology, as described in citation [4], entails the precise division of an input image into either overlapping or non-overlapping blocks, thereby dividing the image into a structured grid. Within the context of this framework, every block is subjected to thorough examination, wherein its feature vector is carefully extracted and analysed for similarities through the utilisation of a similarity index. Although this approach is characterised by its systematic and thorough nature, it serves as the fundamental basis for a specific field of forgery detection. However, it is important to acknowledge that this method does have certain limits.

### SIFT for object detection

Within the ever-evolving realm of digital forensics, the approach of key-point-based forgery detection has emerged as a formidable tool, fundamentally altering our methods of addressing picture manipulation and deceit. Fundamentally, this methodology centres on the systematic process of precisely recognising, delineating, and aligning crucial elements present in an image. This procedure serves as the fundamental factor in the effort to differentiate authentic regions from modified ones, a crucial undertaking in the domain of digital authenticity. The Scale-Invariant Feature Transform (SIFT) algorithm is at the forefront of efforts to enhance the accuracy and effectiveness of key-point-based detection. The fundamental significance of SIFT resides in its remarkable capacity to detect and characterise even the most minuscule elements present in an image, elements that may go unnoticed by the unassisted human visual system. Furthermore, the dedication of the scientific community to advancing knowledge and innovation remains steadfast. Various advanced algorithms, like as the J linkage method, have been developed to enhance the resilience of these systems. The aforementioned developments are propelled by an unwavering commitment to achieving accuracy, a commitment that aims to equal and surpass the inventiveness of individuals engaged in digital forgery [4].

Nevertheless, although these notable advancements, a substantial obstacle emerges—the existence of an upper limit on accuracy that necessitates additional improvement. Despite the great achievements of even the most advanced systems, they still fail to attain the level of perfect precision required, particularly in crucial applications. In light of this ongoing difficulty, a pioneering researcher initiated an endeavour to develop a novel approach, which has the potential to significantly enhance the effectiveness of forgery detection.

This innovative methodology revolves around the effective identification of crucial elements, accomplished by combining the capabilities of two well-established technologies: SURF (Speed Up Robust Feature) and the SIFT detector. The SURF algorithm is widely recognised for its high speed and strong performance, making it a valuable complement to the SIFT detector's ability to extract critical points. The integration of many technologies brings forth a paradigm shift in the field of forgery detection, marked by enhanced precision and robustness.

The feature matching process is facilitated by the utilisation of a hierarchical clustering method, which coordinates a complex and sophisticated study of the data. This methodology reveals patterns and similarities that may escape less complex algorithms, hence yielding noteworthy outcomes [7]. The unique approach employed in this study demonstrates a remarkable accuracy rating of 92.5%, representing a significant milestone in the continuous pursuit of precision. Although the aforementioned accomplishment is certainly praiseworthy, the insatiable desire for constant resilience and exactitude serves as a driving force behind the ongoing quest for additional enhancement.

Within the dynamic and always expanding domain of digital manipulation and forgeries, the relentless desire of achieving flawlessness persists. The achievement of a 92.5% accuracy using this innovative method represents a noteworthy milestone, however it only begins to explore the vast untapped possibilities that lay ahead. There is a significant scope for additional improvements, modifications, and advancements. The researcher's pursuit of advancing forgery detection techniques is an ongoing endeavour, which has the potential to enhance our digital security measures against the elusive tactics employed by contemporary forgers. The unrelenting progression of technology and the increasing sophistication of adversaries have made the search of perfection in forgery detection an urgent endeavour. This quest holds the potential to alter the boundaries of digital forensics in the future.

### Superpixel for the landscape of forgery detection

The key-point-based image forgery detection method developed by Hui-Yu Huang is a significant advancement in the field of digital forensics, demonstrating a notable progress in terms of accuracy and ingenuity. This approach leverages the transformative potential of Helmert transformation and Superpixel segmentation, namely by employing the Simple Linear Iterative Clustering (SLIC) algorithm in a clever manner. Collectively, these constituent elements possess the capacity to reinvent the domain of counterfeit detection, so introducing a novel epoch characterised by enhanced precision and resilience [19].

The core of this methodology is around the principle of Superpixel segmentation, an advanced technique that surpasses conventional pixel-level analysis. Instead of analysing individual pixels independently, this approach reconceptualizes the image as a cohesive assemblage of significant atomic forms. Superpixels, which are atomic zones, serve the purpose of simplifying the complexity of image data and establishing a basis for more precise analysis. The choice to utilise K-Means clustering for the purpose of creating superpixels is a deliberate and calculated decision. This is because K-Means clustering demonstrates exceptional performance in accurately adhering to boundaries, hence effectively retaining the integrity and details of picture regions throughout the segmentation process.

The SLIC algorithm plays a vital role in the important task of colour region detection. The present algorithmic framework expands upon the principles of K-Means clustering by incorporating a neighbor-based clustering methodology that is directed by distance measurements. The implementation of this novel approach effectively reduces the probability of introducing any form of interference or boundary distortions into the initial superpixels, hence enhancing the algorithm's overall resilience. Furthermore, a crucial element in enhancing the effectiveness of the SLIC algorithm entails decreasing the size of the search region in comparison to conventional K-Means clustering techniques. The streamlined technique employed in this study serves to enhance the accuracy of the algorithm and strengthen its ability to withstand sophisticated image alterations.

Hui-Yu Huang's methodology exemplifies the integration of advanced methodologies and a persistent commitment to achieving accuracy in the detection of image counterfeiting. This method explores uncharted terrain in the world of digital forensics by applying Superpixel segmentation and fine-tuning the SLIC algorithm to reimagine image data. It holds the potential to enhance the accuracy and effectiveness of identifying image forgeries.

### Helmert Transformation

The Helmert transformation [6] is a crucial component in the conversion of coordinate systems as it enables the alignment of points inside a common plane. However, it is important to acknowledge that this transformation has inherent limits. Significantly, it has difficulties in the process of consolidating disparate viewpoints into a unified perspective. In order to address this particular obstacle, the methodology adopts the use of affine transformation, harnessing the potential of map coordinate transformations. The utilisation of affine transformation not only preserves the benefits of rotation but also substantially decreases processing complexity, rendering it a practical selection for the current objective.

Nevertheless, despite these achievements, a significant concern persists. Although the method is effective in detecting and preventing several types of forgeries, such as geometric alteration and JPEG compression, it may have weaknesses when dealing with areas in a picture that are smooth, balanced, or have a continuous appearance. The homogeneous nature of these locations poses a barrier to the detection algorithm's capacity to differentiate between authentic and altered areas. This underscores the need for additional research and innovation in this particular domain.

In a related pursuit, as emphasised by the author [7], the attention is redirected from the identification and retrieval of characteristics within a picture to the complex undertaking of identifying non-essential regions. The presence of these regions, which exhibit text that closely matches the original text, presents a distinct and challenging obstacle for conventional feature-based Copy-Move Forgery Detection (CMFD) methods. In light of this perplexing situation, two innovative approaches arise as prospective resolutions, denoted as [9,10].

The scalability of the Scale-Invariant Feature Transform (SIFT) feature across many scales serves as the foundation for these novel approaches. The utilisation of scale-space representation, as implemented through the picture pyramid, plays a crucial role in attaining this desired adaptability. The procedure encompasses a meticulously coordinated sequence of Gaussian smoothing and picture resolution subsampling, ultimately leading to the identification of local extrema by key-point analysis inside the scale-space. Nevertheless, the issue becomes more intricate when the textual content is obscured by a uniformly tinted table, leading to a limited dispersion of crucial information within the impacted areas. As a result, the detection capabilities of traditional copy-move forgery algorithms encounter a deadlock.

The significant advancement is manifested through an innovative methodology, which has the ability to identify duplicate sections that have undergone affine modifications. This represents a substantial progression in the field of forgery detection. Nevertheless, this methodology encounters difficulties when confronted with areas that have seen non-affine alterations, indicating a boundary where additional investigation and advancement are necessary.

Within the ever-evolving realm of digital forensics, these pioneering strategies and inventive procedures signify significant advancements in the continuous struggle against digital counterfeits. As scholars persist in expanding the frontiers of attainable achievements, the forthcoming era exhibits potential for increasingly precise, resilient, and adaptable methods for detecting forgeries, thereby preserving the authenticity of digital content inside a progressively intricate and interconnected global landscape.

Extensive research has been conducted in the field of Copy-Move Forgery Detection, with a significant portion of it being based on SIFT (Scale-Invariant Feature Transform) features, as explained in reference [12]. Although this aspect provided a fundamental basis, other crucial aspects were left unexamined. Significantly, the evaluation of geometric transformations and the real-time assessment of system performance were noticeably lacking in these initial endeavours.

Following this, another researcher embarked on a study in a hitherto unexplored domain, as evidenced in citation [13]. The researchers employed a novel methodology that focused on extracting regions by utilising a correlation map. Although this development was significant, it did not adequately tackle the intricacies associated with affine transformations. Moreover, the assessment of the quantitative reliability of computed geometric transformation parameters has remained an elusive objective, hence necessitating further refinement.

In light of these constraints, the methodology described in citation [11] arose as an innovative resolution, utilising the capabilities of the SIFT algorithm to address the complex issue of geometric transformation in the detection of copy-move fraud. This methodology signifies a substantial deviation from traditional techniques for extracting critical points, since it acknowledges that in instances of forgeries, the duplicated area closely resembles the original image. Therefore, depending exclusively on the extraction of crucial points is inadequate for uncovering probable instances of forgery.

The present study employs a novel methodology that is characterised by a series of sequential steps. The primary focus lies on the extraction of SIFT features and key-point extraction, which serves as the fundamental step in detecting subtle patterns and discrepancies within the image. Following this, the procedure advances to the subsequent stage, wherein the key-points are clustered and meticulously matched, constituting a crucial step in the identification of suspected instances of forgery. Nevertheless, the genuine originality of this methodology becomes evident in its third and ultimate phase, when the assessment of geometric transformation becomes a crucial factor. This essential element disentangles the complex network of alterations that may have been implemented on the manipulated area, allowing the detection system to determine whether the image has indeed undergone copy-move fraud.

The progression from basic SIFT feature-based detection to the current advanced methodology has been characterised by continuous innovation and a steadfast dedication to tackling the complex issues presented by digital forgeries. This methodology not only enhances the precision of counterfeit identification but also enables investigators and forensic specialists to confront the progressively intricate methods utilised by counterfeiters in the era of digital technology. The ongoing pursuit of enhanced accuracy and adaptability in the field of forgery detection is driving the advancement of innovative techniques. These pioneering endeavours are crucial in establishing a future where the preservation of the integrity of digital content is consistently ensured.

### AKAZE for the extraction of descriptor

The thesis discussed in citation [14] undertakes an ambitious endeavour to transform the field of copy-move forgery detection, focusing exclusively on a single image. This innovative project utilises the capabilities of advanced AKAZE (Accelerated-KAZE) features, expanding the limits of accuracy, dependability, and adaptability in detecting modified regions that aim to replicate genuine content [11].

The foundation of this innovative methodology relies on the essential procedure of descriptor extraction, a basic stage that is effectively supported by the Modified Local Binary Pattern (LBP) technology. The aforementioned descriptors are constructed with great care, as they are derived from methodically extracted key-points utilising the AKAZE algorithm applied to the target image. The choice to incorporate AKAZE as the fundamental component of this approach is based on its remarkable capacity to effectively navigate and interpret complex and elaborate modifications that are done to an image.

The primary objective of this project is to advance the field of copy-move forgery detection by integrating state-of-the-art technologies and novel methodologies. The primary objective is to guarantee the reliable authentication and protection of digital content from fraudulent alteration. This study aims to improve our ability to detect digital forgeries that attempt to fool our perception by replicating authentic aspects within a single image, using the skillful application of AKAZE characteristics and the Modified LBP approach [21].

The motivation for the endeavour to achieve high standards in detecting copy-move forgery stems from the growing necessity to counteract advanced methods of digital manipulation. In a contemporary period characterised by the significance of confidence in digital content, the assurance of the integrity and authenticity of images and multimedia emerges as an urgent need. The act of copy-move forgeries, which involves duplicating and relocating sections of an image with the intention of misleading onlookers, poses a considerable obstacle. The limitations of conventional detection approaches become evident when confronted with sophisticated forgery techniques, highlighting the pressing need for novel and accurate solutions.

The incorporation of AKAZE characteristics as the fundamental basis of this study represents a significant advancement. The capability of AKAZE to effectively capture intricate patterns and transformations present in an image, even when subjected to scaling, rotation, and non-linear distortions, is a significant advancement in the field. The system's capacity to detect nuanced but significant discrepancies that suggest fraudulent activities enhances our ability to protect against picture modification.

In addition, the Modified Local Binary Patterns (LBP) technique serves as a valuable supplement to the AKAZE feature extraction method by effectively extracting discriminative descriptors from key-points. These characteristics play a crucial role in differentiating between genuine and altered areas, offering a level of detail that was previously difficult to get. Through a comprehensive analysis of these descriptors, the system is able to reveal the distinct characteristics associated with manipulation, therefore leading to an improvement in the accuracy of detection.

In summary, the research discussed in thesis [14] signifies a notable advancement in the pursuit of dependable detection of copy-move fraud in individual photographs. By combining AKAZE characteristics and the Modified LBP technique, this novel solution enables us to effectively address the always changing nature of digital deception. The utilisation of this technology not only enhances our capacity to detect and prevent instances of forgery, but also preserves the integrity and reliability of digital content in a time where the importance of authenticity cannot be overstated.

### RANSAC for key point distinguish between original and fake image

In order to differentiate between authentic content and probable forgeries, the study utilises the Random Sample Consensus (RANSAC) method. The presented algorithm exhibits a high level of intelligence as it effectively analyses the main points, effectively discerning between genuine components and erroneous associations with a notable level of precision. Through the process of eliminating false positives, the system is able to refine its precision and enhance its ability to withstand different types of image alteration.

In the context of thorough experimental evaluations, this methodology demonstrates considerable potential [16]. This technology demonstrates superior performance compared to previous and concurrent methods in addressing a wide range of obstacles, such as image rotation, blurring, the presence of noise, and the well-known vulnerabilities associated with JPEG compression attacks. Significantly, the notable achievement of the system lies in its exceptional capacity to detect instances of "Object Removal with uniform Background forgery," surpassing other approaches and setting a higher standard for accuracy and dependability.

Nevertheless, the genuine originality of this study resides not alone in its concrete outcomes, but also in its forward-thinking methodology towards the field of digital forensics. This concept presents a novel paradigm that surpasses the primary objective of identifying forgeries and digs into the broader framework of resilience in digital systems.

This approach advocates for the idea that the consideration of robustness should not be a secondary consideration, but rather an essential aspect of every digital system. The presented approach offers a comprehensive perspective on the identification of image forgery, aiming to achieve accuracy while also simplifying system intricacies and minimising computational burden. Essentially, it promotes the endorsement of a comprehensive solution that surpasses the confines of forgery detection and encompasses the entirety of the digital ecosystem.

Significantly, it directly addresses the complex issues presented by digital forgeries. The matters concerning the robustness of the system, the resilience of detection in smooth, symmetrical, and recurrent regions, and the capability to identify forgeries in non-affine transformation regions are thoroughly examined with great enthusiasm and resolve.

Within the ever-evolving realm of digital forensics, this study signifies a significant achievement, a critical juncture where accuracy and resilience intersect to mould the trajectory of counterfeit identification. In the current period, which is marked by a growing dependence on digital media, notable initiatives are being undertaken to establish a secure and reliable digital environment. These efforts aim to safeguard the authenticity and reliability of the content that shapes our interconnected existence.

.

# CHAPTER THREE: RESEARCH METHODOLOGY

### Dataset Search

The selection of a suitable dataset is crucial for ensuring the accuracy and robustness of Copy-Move Forgery detection methods. When selecting a dataset for a machine learning or data analysis endeavour, it is imperative to thoroughly evaluate various crucial factors to ascertain the dataset's appropriateness in relation to your particular requirements and goals. The following are the essential factors to consider:

1. The dataset should exhibit relevance to the problem at hand in order to effectively address the research objective. It is imperative to ensure that the data encompasses the pertinent aspects and features necessary for answering the study question or resolving the specific situation at hand.
2. Data Quality Assessment: Evaluate the quality of the data. The dataset should be examined for the presence of missing values, errors, outliers, and inconsistencies. The utilisation of data of inferior quality may result in outcomes that are biassed or erroneous.
3. Dataset Size: It is important to take into account the magnitude of the dataset. A larger dataset has the potential to enhance the accuracy of models, particularly when dealing with intricate situations. Nevertheless, this approach necessitates a greater allocation of computer resources and may result in extended processing times.
4. The assessment of class or category balance in classification tasks is essential. The presence of imbalanced datasets might lead to the development of biassed models, underscoring the importance of guaranteeing an adequate quantity of samples for each class or category.
5. Data Diversity: It is imperative to ensure that the dataset exhibits diversity and accurately represents the real-world scenarios that the model is intended to be applied to. The absence of diversity may result in models that exhibit high performance on the dataset but demonstrate failure when applies in practical scenarios.
6. Data Source and Collection Method: Gain an understanding of the data collection process and the specific source from which the data was obtained. The generalizability of a model might be affected by biases present in the methodology or sources used for data collecting.
7. Data Accessibility: Determine whether the dataset is freely accessible or necessitates certain rights or licencing. It is vital to ascertain if you possess the necessary authorization to utilise the data for your project.
8. Data Updates: It is important to assess whether the dataset under consideration is static or subject to regular updates. In certain contexts, the availability of current data is of utmost importance.
9. Benchmark Datasets: In certain instances, it can be advantageous to use benchmark datasets that are extensively employed within the discipline, as they enable comparisons with prior research.
10. Bias and Fairness: It is imperative to acknowledge the presence of potential biases within the dataset and critically evaluate if these biases may be perpetuated or introduced into the models being utilised. Implement measures to mitigate bias and foster equity in your analysis.

The selection of a suitable dataset is a critical component of our research, since it has a direct influence on the integrity and reliability of our findings. In the context of Copy-Move Forgery detection, the selection of an image dataset is of utmost importance, as it must possess both efficiency and a faithful representation of real-world circumstances. After conducting a thorough evaluation of multiple criteria, we have made the decision to collaborate with the CASIA V2 dataset.

The CASIA V2 dataset, which was introduced by Dong et al. (year), is a highly regarded and widely utilised dataset in the field of image-related research. CASIA V2 is a dataset that has been purposefully created for the classification of forgery. It consists of a total of 4795 photos, which can be further categorised into 1701 authentic images and 3274 forged images. The dataset presented provides a wide array of photos, encompassing both genuine and modified information in a balanced manner. Consequently, it serves as an optimal selection for our research endeavours.

The utilisation of CASIA V2 ensures that our methodology undergoes thorough examination on a dataset that is widely recognised and frequently utilised within the domain of picture forensics. The resource's widespread usage and high level of popularity in previous research endeavours render it a highly desirable asset for the purposes of training, testing, and assessing computer vision algorithms. In general, CASIA V2 provides a strong basis for our research endeavours, facilitating the execution of rigorous and significant experiments within the realm of Copy-Move Forgery detection.

The act of tampering with images is a prevalent and enduring issue that has spanned several decades. In light of the ongoing global transition towards the digital era characterised by technological advancements and widespread internet usage, the imperative to tackle this issue becomes progressively paramount. The issue of copy-move forgeries is a prominent method of manipulating images, and the purpose of this presentation is to propose a hybrid solution to address this challenge.

A plethora of remedies have been posited over the course of time to effectively tackle this matter, and their efficacy has been substantiated in recent times. In the context of detecting copy-move forgeries, a hybrid solution has been devised that effectively combines the merits of two separate methodologies. In the initial phase, an unsupervised methodology was utilised to detect occurrences of tampering inside photographs. Following this, I further expanded upon this methodology by integrating supervised learning methodologies.

The proposed hybrid methodology integrates the benefits of unsupervised and supervised methods in order to improve the precision and resilience of copy-move fraud detection. Through the implementation of a complete approach, my objective is to make a meaningful contribution to the continuous endeavours aimed at addressing the issue of image manipulation within our progressively digitalized and networked global society.

### Implemented Technique

The proposed methodology for detecting image counterfeiting is a two-fold approach, incorporating both unsupervised and supervised techniques. The unsupervised part of image analysis involves the exploration of hidden patterns and structures within datasets, without the need for explicit labels or goal values. The motivation behind this investigation stems from the algorithm's capacity to identify intrinsic connections among data points, traits, or features. The primary unsupervised tasks encompass clustering, dimensionality reduction, density estimation, anomaly detection, and generative modelling. Hybrid Copy-Move forgery detection employs particular unsupervised techniques, such as SURF, SIFT, Agglomerative Clustering, and RANSAC, to effectively detect occurrences of image tampering.

Concurrently, the supervised technique functions by utilising datasets that have been labelled, meaning that each data point is assigned a known label. This labelling process enables the algorithm to be trained in order to produce predictions or classifications based on the input attributes. The supervised process involves several essential stages, namely dataset preparation, model development (employing convolutional neural networks or CNNs), training, evaluation, and iterative improvement. The hyperparameters, including the number of training epochs and batch size, are set, and the Adam optimizer is utilised to minimise the Binary Cross-Entropy loss during the training process.

The assessment of this technique entails the examination of model performance by the utilisation of diverse metrics, such as precision, recall, F1 score, and accuracy, using a specifically designated validation dataset. Moreover, ROC curves are utilised to visually represent the balance between the rates of correctly identified positive instances and incorrectly identified negative instances. In parallel, confusion matrices offer vital insights into the effectiveness of classification performance.

This hybrid approach combines unsupervised approaches for feature extraction with supervised convolutional neural networks (CNNs) for picture classification. The objective is to provide a complete and efficient solution for detecting image forgeries. This approach ensures both accuracy and robustness in accurately identifying modified images.

### Architectural Diagram

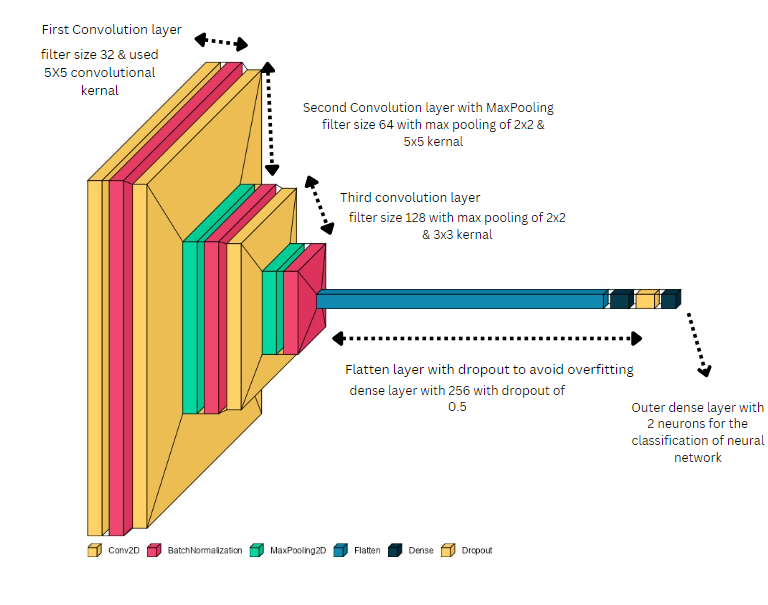


Figure - Custom CNN Model

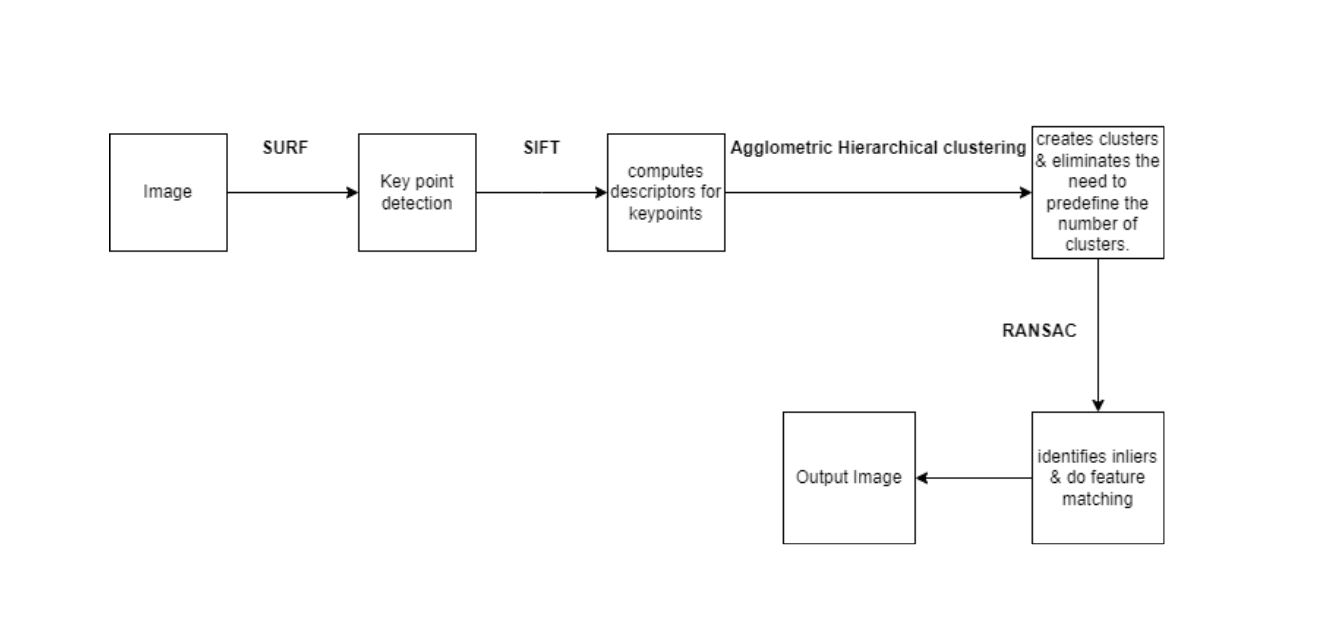


Figure - Unsupervied approach

### Unsupervised Approach

Unsupervised learning constitutes a basic subfield within the realm of machine learning and data analysis, with a primary emphasis on the investigation and extraction of concealed patterns and structures inherent in datasets. Unsupervised learning distinguishes itself from other machine learning paradigms, such as supervised learning, by operating within an environment where data points do not include explicit labels or target values.

In a conventional supervised learning setting, the algorithm is presented with a dataset that is annotated, indicating that each instance is accompanied by an explicit indication of its intended output or category. In the context of a spam email classifier, individual emails are assigned categorical labels denoting their classification as either "spam" or "non-spam."

In contrast, unsupervised learning functions without the presence of such explicit direction. This scenario might be likened to presenting the algorithm with a puzzle, while withholding information regarding the desired final image. The primary objective of the algorithm is to independently identify and analyse patterns, similarities, and underlying structures inherent in the dataset. This implies that the system must depend on the intrinsic connections among data points, traits, or features in order to interpret the information it is given.

Unsupervised learning algorithms are capable of performing a wide range of tasks, which encompass:

1. Clustering algorithms aim to group data points together by identifying shared traits or proximity in the feature space. Clusters are indicative of inherent groups within the dataset, although the algorithm lacks prior knowledge of the labels or interpretations associated with these clusters.
2. Dimensionality reduction is a methodology employed in the context of high-dimensional datasets, wherein unsupervised techniques are utilised to decrease the number of variables while preserving crucial information. The utilisation of this approach facilitates the process of data visualisation, expedites computational tasks, and aids in the elimination of extraneous or repetitive elements.
3. Density estimation is a task within unsupervised learning that involves estimating the probability density function of a given dataset. This process is particularly valuable for statistical analysis and the generation of synthetic data points to facilitate simulations.
4. Anomaly detection is a technique used to identify data points that exhibit substantial deviation from the established norm. These anomalies may indicate potential inaccuracies, fraudulent activities, or atypical occurrences.
5. Generative modelling refers to the ability of unsupervised learning algorithms to construct models that effectively capture the underlying distribution of a given dataset. These models have the capacity to produce novel data samples that closely mimic the characteristics of the original dataset. The aforementioned techniques find utility in the domains of data augmentation, image synthesis, and natural language production.

Unsupervised learning is a very adaptable technique utilised for the purpose of data exploration and comprehension, particularly in scenarios involving unstructured or unlabeled data. Machine learning is extensively utilised throughout many fields, including but not limited to data analysis, natural language processing, computer vision, recommendation systems, and other topics. Unsupervised learning plays a crucial role in contemporary data science and machine learning by autonomously identifying patterns and structures within intricate datasets, hence yielding useful insights.

The unsupervised model developed for hybrid Copy-Move forgery detection incorporates four important methods to effectively detect instances of picture alteration. The algorithms encompassed in this set are SURF, SIFT, Agglomerative Clustering, and RANSAC. Each of these algorithms plays a pivotal role in augmenting the precision and efficacy of the forgery detection process. The following information provides an overview of the algorithms and their operational mechanisms within the model:

### *Surf*

The SURF algorithm, known as Speeded-Up Robust Features, is a crucial computer vision methodology that holds significant importance in diverse applications. It provides a flexible and effective approach for tasks related to image analysis and processing. The method known as SURF, which was developed in the seminal 2006 paper titled "SURF: Speeded Up Robust Features" by Herbert Bay, Tinne Tuytelaars, and Luc Van Gool, has emerged as a fundamental tool within the domain of computer vision.

The primary focus of SURF revolves around the identification and characterization of crucial interest points, also known as keypoints, inside an image. The aforementioned keypoints possess distinctive and exclusive attributes inside a picture, rendering them essential for a diverse array of applications, spanning from object detection to image stitching and beyond. The distinguishing characteristic of SURF lies in its exceptional capability to identify keypoints across various scales and orientations, hence assuring resilience in the presence of variations in object size, viewpoint, and rotation.

The efficiency of the SURF algorithm is attributed to its utilisation of novel methodologies such as integral pictures and box filters. The utilisation of computational approaches facilitates the efficient identification and characterization of keypoints, resulting in a notable decrease in the temporal and material resources needed for processing. Consequently, the Speeded Up Robust Features (SURF) algorithm has gained recognition for its rapidity and computing efficacy, rendering it a favoured option for applications that require real-time processing and have limited computer resources.

One notable characteristic of SURF is its ability to maintain scale invariance, enabling it to identify keypoints across different scales within an image. The aforementioned capacity is of great value when encountering objects or settings that may exhibit variations in size or distance as seen by the camera. Moreover, the Speeded Up Robust Features (SURF) algorithm exhibits rotation invariance, enabling it to detect and describe keypoints in a picture regardless of the object's orientation. The utilisation of both scale and rotation invariance in SURF renders it a resilient option for applications in which objects may exhibit varying sizes and orientations.

### *SIFT*

The SIFT algorithm, which was first presented by David G. Lowe in his influential paper titled "Distinctive Image Features from Scale-Invariant Keypoints" in 2004, has had a significant impact on the domain of computer vision. The SIFT algorithm has gained significant recognition due to its ability to adapt to various image processing and computer vision applications, particularly in situations where retaining scale and rotation invariance is crucial.

Fundamentally, the Scale-Invariant Feature Transform (SIFT) has brought about a significant transformation in the manner in which we detect and characterise features within images. The process commences with the identification of keypoints, which are specific points within a picture that possess special characteristics. These important aspects form the fundamental basis for a diverse array of computer vision applications, encompassing object recognition, picture matching, and image stitching, among others.

One notable characteristic of the Scale-Invariant Feature Transform (SIFT) is its capacity to effectively manage fluctuations in scale. The accomplishment is attained by employing a scale-space pyramid, which is a hierarchical depiction of the image where each level corresponds to a distinct scale. The SIFT algorithm employs Gaussian blurring and downsampling methods to generate several scales, so ensuring that keypoints are identified as local extrema in the difference-of-Gaussian (DoG) pictures. The utilisation of a multi-scale method enables the SIFT algorithm to effectively detect and recognise features regardless of their size. This characteristic empowers the algorithm to perform equally well in identifying both huge items in close proximity and small things situated at a distance.

The commitment of the Scale-Invariant Feature Transform (SIFT) algorithm to preserving invariance is not limited to scale, but also encompasses rotation. Every keypoint possesses a prominent orientation, which is determined through a thorough examination of the gradient directions within the immediate image patch around the keypoint. The purpose of this orientation assignment is to ensure the preservation of critical features, irrespective of the object's rotational orientation inside the image. The distinctive characteristic that distinguishes SIFT is its ability to maintain both scale and rotation invariance.

The inherent strength of the Scale-Invariant Feature Transform (SIFT) rests in its capacity to produce descriptors for every detected keypoint. The descriptors serve as concise representations of the picture patch in the immediate vicinity, including the fundamental information necessary for the identification and correlation of features. The generation of these descriptors involves a detailed analysis of the gradient magnitude and direction at multiple places inside the patch by the SIFT algorithm. The resulting output is a vector that represents the distinctive visual characteristics of the feature. These descriptors form the basis for effective feature matching and recognition between images.

Although the resilience and accuracy of SIFT in addressing scale and rotation changes are widely recognised, it is crucial to realise that its computing efficiency may not always be optimal, especially in situations with limited resources or real-time applications. However, the significant impact of SIFT on the field of computer vision cannot be overemphasised. The innovative ideas and approaches of this approach have had a significant impact, influencing the development of feature recognition and description methods and contributing to breakthroughs in various applications such as robotics, augmented reality, and image stitching, among others. The SIFT algorithm, known for its ability to maintain scale and rotation invariance, continues to be an important tool in the field of computer vision. Its effectiveness serves as evidence of the lasting influence of pioneering research in this domain.

### *Aglometric clustering*

Agglomerative Hierarchical Clustering, also referred to as Hierarchical Clustering, is a versatile and extensively utilised technique in the fields of data analysis and machine learning. This approach, which falls under the category of agglomerative clustering, creates clusters by iteratively merging data points or smaller clusters. One notable characteristic of Hierarchical Clustering is its distinctive ability to arrange data points in a hierarchical manner, resulting in the formation of a tree-like structure that effectively reflects the grouping of the data at various degrees of detail.

The process of Agglomerative Hierarchical Clustering follows a systematic unfolding of mechanics. The process commences with an initialization phase, during which every individual data point is regarded as a separate cluster. As a result, the quantity of clusters at this particular step is equivalent to the quantity of data points being examined.

The fundamental nature of the method becomes apparent throughout the iterative merging procedure. Clusters are methodically combined in a sequential manner. The evaluation of the proximity level across clusters is conducted by employing a selected distance measure or linkage criterion. The determination of distances between clusters is determined by metrics such as Euclidean distance and Ward's linkage. It is crucial to note that the selection of a connection criterion has a substantial impact on the results of clustering. The three common linkage approaches in clustering analysis are single linkage, complete linkage, and average linkage. Single linkage aims to minimise pairwise distances across clusters, while complete linkage strives to maximise pairwise distances. Average linkage calculates the average of all pairwise distances.

As the merging process of clusters continues, a complex hierarchical structure emerges, which is visually depicted as a dendrogram. The dendrogram exhibits a structural resemblance to a tree diagram and serves to clarify the chronological order of cluster unions. At the lowest hierarchical level of the dendrogram, each data point is represented as a distinct cluster. As the dendrogram is traversed upwards, clusters gradually merge until they eventually converge into a one comprehensive cluster that encompasses all the data points.

The process of Agglomerative Hierarchical Clustering is considered complete when a predetermined stopping criterion has been met. The selection criteria for this can manifest in other ways, such as a predetermined quantity of desired clusters, a specific threshold distance, or any other condition that aligns with the objectives of the challenge. After the completion of the clustering procedure, the resultant clusters are obtained by performing a cut at a suitable level on the dendrogram, so producing the definitive clusters.

The attractiveness of Agglomerative Hierarchical Clustering stems from its several advantages. First and foremost, it provides a hierarchical depiction of clusters, so affording data analysts the flexibility to investigate data at different levels of detail. In contrast to certain alternative clustering techniques, such as k-means, this method eliminates the requirement of predefining the number of clusters. Moreover, this approach enables analysts to retrospectively determine the optimal number by carefully examining the dendrogram. In addition, the dendrogram plays a crucial role in interpretation by providing useful insights into the interconnections between data points and clusters. This aids in making educated decisions about determining the most suitable number of clusters.

Nevertheless, it is essential to recognise the processing requirements associated with Agglomerative Hierarchical Clustering, especially when employed on large datasets. The computational load is particularly evident when utilising linkage methods such as complete linkage or single linkage, as they require calculating pairwise distances for all data points. In addition, it is important to note that the selection of the linkage method and distance metric can have a significant impact on the results of clustering analysis. Therefore, it is crucial to carefully evaluate and deliberate on these factors.

### *Ransac*

The Random Sample Consensus (RANSAC) method, which stands for Random Sample Consensus, is a very influential and extensively utilised technique in the domains of computer vision, image analysis, and robust statistical estimation. The fundamental objective of this mission is to effectively and precisely estimate the parameters of a model using a given dataset, particularly in cases where a substantial amount of the data is affected by outliers or errors. The algorithm initiates its operation by randomly selecting a minimal subset of data points from the input dataset. This subset is specifically designed to align with the number of parameters that need to be estimated by the model. For example, in the context of fitting a line, two locations are selected at random in order to ascertain crucial line parameters such as slope and intercept.

After the process of subset selection, the algorithm proceeds to estimate the model parameters using the subset that has been manually chosen. In the specific context of linear regression, the algorithm computes the equation of the optimal line of best fit by utilising the selected data points. Afterwards, the algorithm evaluates the degree to which this estimated model corresponds with the complete dataset. In this assessment, every individual data point is analysed to establish its adherence to the model based on a predetermined threshold. Data points that fall inside the threshold are classified as inliers, while those that deviate significantly beyond the threshold are classified as outliers.

The aforementioned procedure of iteration, consensus evaluation, model refining, and eventual model selection is repeated for a predetermined number of iterations or until a pre-established termination condition is satisfied. The primary goal is to determine the model that exhibits the most comprehensive consensus set, indicating the highest number of inliers throughout all iterations. The resulting model is widely regarded as the most suitable representation of the data, as it successfully incorporates and minimises the impact of outliers.

The significance of the RANSAC algorithm becomes prominent in scenarios when datasets are afflicted by noise or outliers, leading to reduced effectiveness of conventional least squares techniques. The method demonstrates extensive use across a diverse range of fields. The algorithm is utilised for various tasks, including the fitting of 2D and 3D lines or planes to point clouds, the estimation of homography for accurate picture alignment in computer vision applications, and the matching of features where it can effectively find corresponding features in images, even when there are misalignments and outliers present.

Although RANSAC is widely recognised for its capability to yield resilient and precise answers in the presence of data noise, it incurs heightened computational complexity as a result of its iterative characteristics. However, the RANdom SAmple Consensus (RANSAC) algorithm continues to be a highly valuable tool in numerous disciplines where the robust estimate of model parameters is of utmost importance. It guarantees the attainment of precise outcomes even in situations where the quality of data is impaired due to the presence of outliers or errors.

### Supervised Approach

A supervised approach refers to a machine learning paradigm in which an algorithm is taught using a labelled dataset, wherein each data point is linked to a specified target or outcome. In the context of supervised learning, the algorithm acquires the ability to generate predictions or classifications by leveraging the input characteristics and their associated labels.

The following are the fundamental attributes and procedures associated with a supervised approach:

1. The utilisation of labelled data is a fundamental aspect of supervised learning, wherein a dataset is initially provided, comprising individual data points that encompass distinct features or properties, alongside their matching goal or label. The label corresponds to the intended outcome or classification linked to a certain data point. In the context of a spam email classifier, individual emails are assigned categorical labels denoting their classification as either "spam" or "non-spam."
2. During the training phase, the algorithm undergoes training using the labelled dataset. The machine learning model leverages the input information to acquire knowledge about patterns, relationships, or decision boundaries, hence facilitating accurate predictions or classifications.
3. Model Construction: Utilising the provided training data, the programme constructs a predictive model. The selection of a particular model is contingent upon the nature of the problem being addressed. Supervised learning encompasses a range of prevalent models, such as decision trees, support vector machines, neural networks, and linear regression, among other notable examples.
4. Prediction and inference are possible outcomes once the model has undergone training. These outcomes involve the ability to make predictions or classifications on previously unknown data. The aforementioned predictions are derived from the patterns and relationships that the model has acquired through the analysis of the training data.
5. Evaluation: The model's performance is assessed by the utilisation of diverse measures, which are contingent upon the specific characteristics of the problem at hand. Prominent evaluation metrics encompass accuracy, precision, recall, F1-score, and mean squared error, among other measures.
6. The iterative process involves refining the model's performance by the adjustment of hyperparameters, utilisation of alternative algorithms, or acquisition of additional labelled data, in cases where the model's performance is deemed unsatisfactory. The aforementioned procedure frequently follows an iterative approach, aiming to enhance the precision and ability of the model to generalise when presented with novel data.

The Error Level Analysis (ELA) technique Initially, the deep learning library TensorFlow is imported. In addition, we import essential libraries for data loading, data visualisation, and the sklearn library. Scikit-learn offers techniques for supervised learning, which involve the classification of data into pre-established categories or classes.

Next, we construct a function known as ELA (Error Level Analysis). The programme is responsible for the loading and distinction of images. This study focuses on the provision of image path and quality, as well as the normalisation and enhancement of image brightness. The latter phase aims to improve the visual depiction of variations within the image. Next, we proceed to access an image file and implement Error Level Analysis (ELA) on it. The specific image file path and desired quality parameters are provided for this purpose.

### *Dataset Prepration*

In the process of preparing the dataset, it is customary to maintain the image dimensions at 128 by 128 pixels. In this task, we will develop a method that utilises the ELA (Error Level Analysis) function to manipulate the intensity, size, and quality of an image. The process involves resizing and flattening the image, followed by normalising the resulting output. Then, two variables, X and Y, are declared. In X, all the features that Y possesses are present. Additionally, X encompasses all the labels associated with Y. There are two possible values for variable Y, namely 0 and 1. The value of 0 is indicative of a fabricated image, while a value of 1 signifies an authentic image.

The selection of the images of authentic and manipulated was conducted in a random manner. Both the actual and tempered values are 2100. Next, we proceed to visualise the data in order to determine whether the results are incorrect or acceptable. Next, a process of one-hot encoding is applied to the data. In this context, we are presented with two distinct labels, labelled as 0 and 1, which cannot be definitively classified as either real or fake. Hence, we categorise them as either 0 or 1. Next, the image is subjected to a process of reshaping.The model utilised in our study incorporates four variables, namely the number of images, height, width, and channel. Next, we conducted the Train test and divided the dataset using an 80:20 ratio. In this context, the sklearn library is utilised and afterwards invoked. Next, we proceed to output the X\_train, Y\_train, X\_val, and Y\_val datasets, utilising a test size of 0.2. As a result, the testing dataset consists of 3331 photos, while the validation dataset comprises 883 images.

### *CNN*

The CNN model incorporates a convolution block, batch normalisation, and max pooling. The convolutional layers are utilised in this CNN model. In the context of convolutional layers, it is customary to employ a "2D convolutional layer" for the purpose of image processing tasks. In the context of convolutional layers, distinct numbers of filters are employed to identify various patterns or features within the input data. Next, we assigned the convolutional size for each layer. The padding mode utilised during the convolution procedure has been defined as "valid". The term 'valid' padding refers to the absence of any padding being applied to the input image, which in turn leads to a smaller output feature map when compared to the 'same' padding technique. The activation function employed for the Model is the rectified linear unit (ReLU). The acronym ReLU denotes Rectified Linear Unit, which is a widely employed activation function in neural networks and deep learning models. The non-linear activation function under consideration is a straightforward yet efficient mechanism that imparts non-linearity to the model. The rectified linear unit (ReLU) activation function is mathematically stated as follows: The function f(x) is defined as the maximum of 0 and x. The given equation represents the relationship between the input, denoted as x, and the output, denoted as f(x), of the activation function. In the case where the input variable x is greater than zero (x > 0), the resulting output is equivalent to the function f(x) = x. In the case where x is a negative value (x ≤ 0), the resulting output will be zero (f(x) = 0). The Rectified Linear Unit (ReLU) function is a mathematical operation that effectively substitutes any negative values in the input with zero, while preserving positive values without alteration. The incorporation of non-linearity into the model is of utmost importance as it allows neural networks to acquire intricate patterns and representations within the given data.

Additionally, the function of max pooling is also performed within it. The process involves applying a 2x2 max pooling operation on the input feature map, resulting in a reduction of its spatial dimensions. This operation selectively retains the most significant information, which is then utilised by succeeding layers in the neural network. The utilisation of this particular layer is frequently observed in tandem with convolutional layers to establish a hierarchical procedure for extracting features in convolutional neural networks (CNNs).

The final stage of the convolutional layer involves the implementation of "Batch Normalisation." Batch normalisation is a widely employed technique in the realm of deep neural networks, aimed at enhancing the stability of training and expediting the process of convergence. The process involves normalising the activations of the preceding layer through the subtraction of the batch mean and division by the batch standard deviation. This technique aids in mitigating challenges such as the occurrence of vanishing gradients throughout the training process. Batch normalisation layers are frequently incorporated into deep neural networks following convolutional or fully connected layers in order to standardise the activations.

The network comprises a series of convolutional layers.

1. The first convolutional layer is a fundamental component of a neural network architecture. The initial layer consists of 32 filters, each employing 5x5 convolutional kernels. The convolutional operation is performed with 'valid' padding, and the rectified linear unit (ReLU) activation function is applied. Subsequently, a batch normalisation layer is incorporated into the network to enhance the stability of the training process. The utilisation of these two layers in tandem is a common practise for the purpose of processing picture data inside a deep learning framework.
2. The second convolutional layer is comprised of a convolutional layer with 64 filters, which are activated using the Rectified Linear Unit (ReLU) function. This is then followed by max pooling with a 2x2 kernel and batch normalisation. The purpose of this block is to extract and process features that are at a higher level from the supplied data. It is a prevalent practise to employ the stacking of numerous such blocks in order to construct a deep convolutional neural network, particularly for tasks such as image categorization.
3. The third convolutional layer is composed of a convolutional layer with 128 filters. Each filter uses a 3x3 kernel and applies the Rectified Linear Unit (ReLU) activation function. This configuration allows for the extraction of complex features from the input data. Subsequently, a max-pooling layer is employed with a window size of 2x2 to execute downsampling on the feature map, so successfully decreasing its spatial dimensions. In order to improve the stability of training and expedite the convergence process, a batch normalisation layer is incorporated, which serves to normalise the activations inside each mini-batch

### *Flatten and fully connected layers*

Following the convolutional layers, a flatten layer is employed, which is subsequently connected to dense layers and include a dropout function. Following the flattening process, a dense layer is implemented, consisting of 256 neurons. Every individual neuron inside this particular layer is intricately linked to each and every element included within the flattened vector originating from the preceding layer. The activation function employed in this dense layer is ReLU (Rectified Linear Unit), which brings non-linearity into the network by producing the input for positive values and zero for negative values. The dense layer, when utilising the rectified linear unit (ReLU) activation function, is capable of acquiring intricate patterns and establishing correlations within the given dataset. Following the inclusion of the dense layer, a dropout layer is incorporated for the purpose of regularisation.The term "dropout(0.5)" denotes a dropout rate of 0.5, indicating that around 50% of the neurons in the preceding dense layer will be randomly deactivated or "dropped out" during each training batch. The utilisation of dropout in neural networks serves the purpose of mitigating overfitting by diminishing the dependence on individual neurons, hence fostering the acquisition of more resilient properties by the network. In the domain of neural networks, the term "overfitting" pertains to a prevalent predicament encountered in machine learning, wherein a model exhibits great performance on the training dataset but has subpar performance when presented with unseen or novel data. Overfitting is a phenomenon that arises when a model has the ability to memorise the noise and quirks included in the training data, rather than effectively collecting the fundamental patterns and generalizable characteristics. The utilisation of dropout layers serves as a regularisation strategy that is employed to mitigate the issue of overfitting. The functioning of this mechanism involves the random deactivation, also referred to as "dropping out," of a specific proportion of neurons in each training iteration. The dropout rate is defined as the fraction of neurons that are deactivated, often denoted by a value ranging from 0 to 1, indicating the proportion of neurons to be dropped out.

### *Output layer*

The last layer being utilised is the output layer. Next, we proceed to implement a dense layer with two neurons, as this configuration will effectively represent the binary values of 0 and 1. The activation function employed for the activation of this function is softmax. The softmax function is frequently employed in the output layer of classification neural networks. The process involves converting the initial output scores (logits) of the network into a probability distribution across the various classes. In the context of binary classification, the process involves the conversion of logits into class probabilities for the two distinct classes. This conversion is carried out in a manner that guarantees the summation of probabilities to equal 1. Subsequently, construct the model and generate a summary.

### *Hyperparameter Setting*

Hyperparameters are utilised to optimise the performance of a model. In the context of hyperparameter tuning, the number of epochs is set to 30. The variable in question denotes the quantity of training epochs, which signifies the number of iterations the model will undergo throughout the complete training dataset during the training process. The batch size used in this experiment was 32. The batch size parameter is responsible for specifying the quantity of samples utilised in both the forward and backward passes throughout the training process. A batch size of 32 signifies that 32 individual samples will be collectively processed before to the update of the model's parameters. Finally, the metrics for the outcome are determined.

### *Optimizer*

An optimizer object for training a machine learning or deep learning model. The Adam optimizer is employed, utilising an initial learning rate (init\_lr) and a learning rate decay approach to regulate the adjustment of the learning rate throughout the training process. The optimisation of the learning rate and learning rate decay is crucial for achieving effective training and convergence of neural networks. The Adam optimizer is a commonly employed optimisation method in the fields of machine learning and deep learning owing to its adaptive learning rates, efficacy, and resilience. The Adam optimizer is frequently used as the default choice for optimising the training of neural networks and has attained the status of a standard optimisation algorithm in numerous deep learning frameworks, such as TensorFlow and Keras.

Following the completion of the previous step, the model is compiled. In order to achieve the desired compilation objective, the binary\_crossentropy function is employed. The objective during the training process is to minimise the Binary Cross-Entropy loss. The optimisation approach employed in this context incentivizes the model to generate predictions that are both confident and accurate, hence aligning with the true labels. As the model's performance increases, there is a corresponding decrease in the loss function, indicating an enhanced ability to differentiate between the two classes in the binary classification task. Subsequently, we implemented the EarlyStopping function, which serves the purpose of terminating the training process prematurely in the event of unfavourable progress, hence mitigating the potential for further loss.

Next, we proceed with the model training phase, during which we employ the early stopping function. The training process was conducted for a duration of 30 epochs. Subsequently, the programme will proceed to display the output. The results under evaluation pertain to the testing data.

The test result prediction is obtained by employing X validation, where the input is compared with the actual label. The outcomes are obtained.

### *Accuracy of the model*

Subsequently, the Receiver Operating Characteristic (ROC) analysis was employed. The Receiver Operating Characteristic (ROC) curve is a graphical instrument that is extensively employed as an evaluation metric in the field of machine learning and classification tasks, with a special focus on binary classification. The purpose of this tool is to evaluate the effectiveness of a classification model by presenting the balance between its sensitivity (true positive rate) and specificity (false positive rate) at various decision thresholds. Please generate and display the confusion matrix.

# CHAPTER FOUR: FINDINGS (Or RESULTS)

### Configuration Settings

For our proposed method we have used the following basic configurations.

Programming Language = Python 3.9

Forgery type: Copy-Move Forgery

Framework = TensorFlow and Keras

Library = numpy, sklearn, matplotlib,

Dataset = CASIA2

Model = Custom CNN model

### Results of these applied techniques

### *Unsupervised Approach results*

In order to evaluate the efficacy of our algorithms, we will select an image to serve as a test case and assess whether it yields accurate findings. In order to evaluate the detection capabilities, a tempered image was utilised. Specifically, a portion of the tempered image was incorporated into the original image to assess its detectability.

### *Surf*

In the context of image forensics, the Surf method is employed to discover instances of Copy-Move Forgery by analysing a modified version of the original image. The image displays a green square that is capable of identifying both the authentic and manipulated regions.

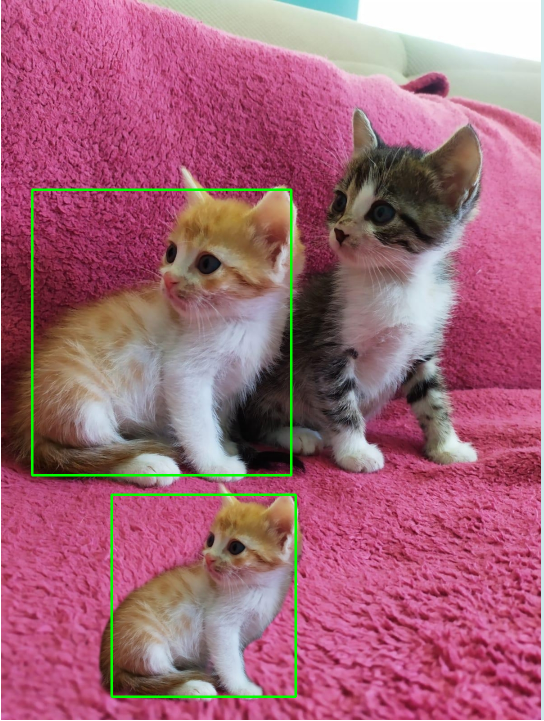


Figure - SURF Accuracy

### *SIFT*

For SIFT we are using we are using blue color to represent the algorithm is applied.

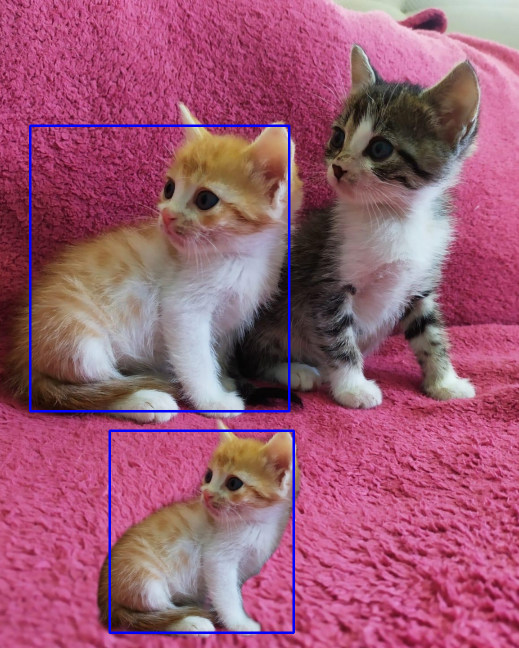


Figure - SIFT Accuracy

### *Aglometric Clustering*

For this algorithm we define the black color. With the green dots telling the clustering point where it sees the same tempered object.

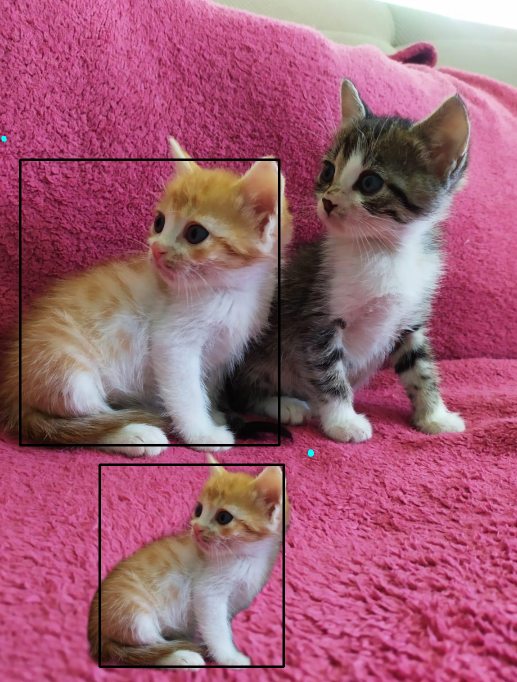


Figure Aglometric Clustering Accuracy

### *RANSAC*

For ransac we are using black color only to detect the object that is tempered.



Figure - Accuracy of RANSAC

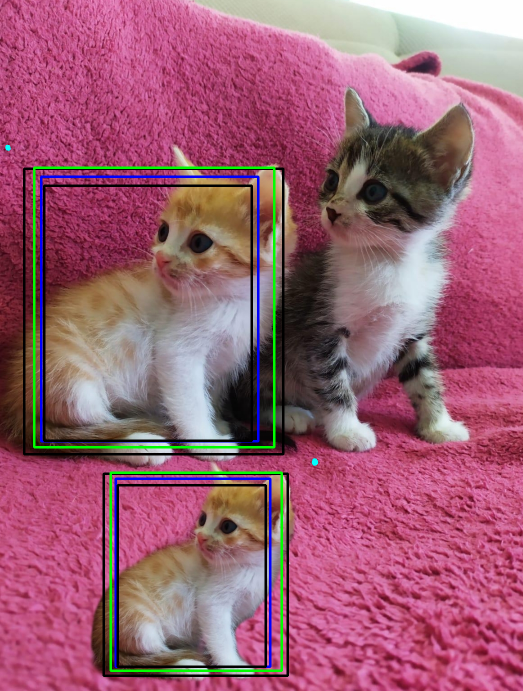
Using each of the algorithms in parallel with one another. In order for us to view the fake.

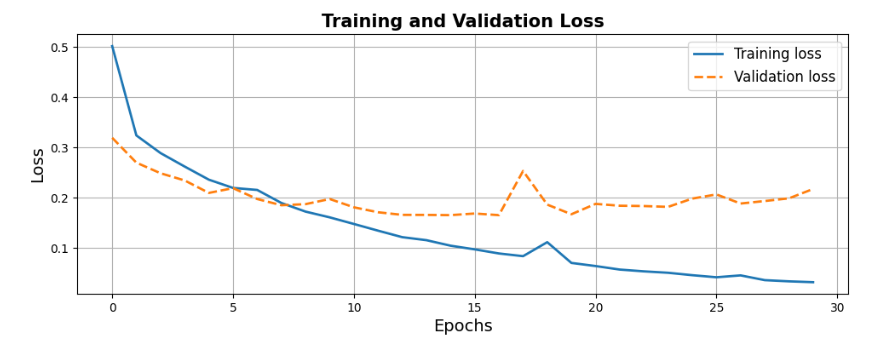
Figure - Applying all the above unsupervised algorithms

In the concluding phase, our unsupervised approach was implemented and seen to yield satisfactory results, successfully detecting instances of forgeries. The Hybrid model employed for detecting Copy-move forgery exhibits satisfactory performance.

### Supervised Learning approach Results

### *Graph Validation loss*

Figure - Graph of validation

A validation loss graph depicts how well a machine learning model generalizes to new data over training epochs. It shows the relationship between the model's error on a validation set and the number of training iterations. The graph helps identify the point of optimal generalization and potential issues like overfitting, guiding decisions on when to stop training or adjust the model for improved performance on unseen data.

### *Graphs for Accuracy*

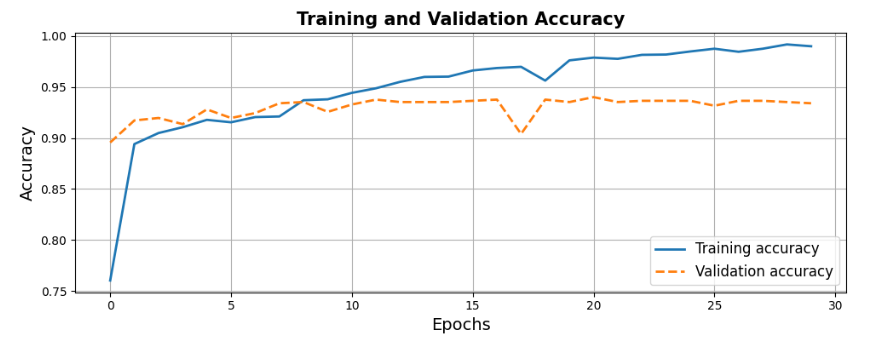
  
An accuracy graph tracks a machine learning model's classification performance over training epochs. It plots accuracy against the number of iterations, helping assess how well the model is learning. Increasing accuracy signifies improved performance, guiding decisions on training duration and adjustments for optimal classification outcomes.

Figure 9- Graph of Accuracy

### *Graphs for Precision*

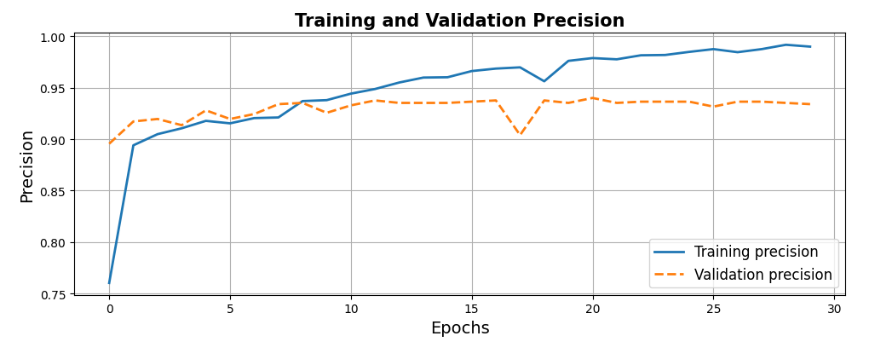


Figure - Graph of precision

A precision graph tracks the precision metric of a machine learning model during training. It plots precision against the number of epochs, providing insights into the model's accuracy in positive predictions. Monitoring this graph helps optimize the model's performance by minimizing false positives, contributing to the effective development and evaluation of classification models.

### *Graphs for Recall*

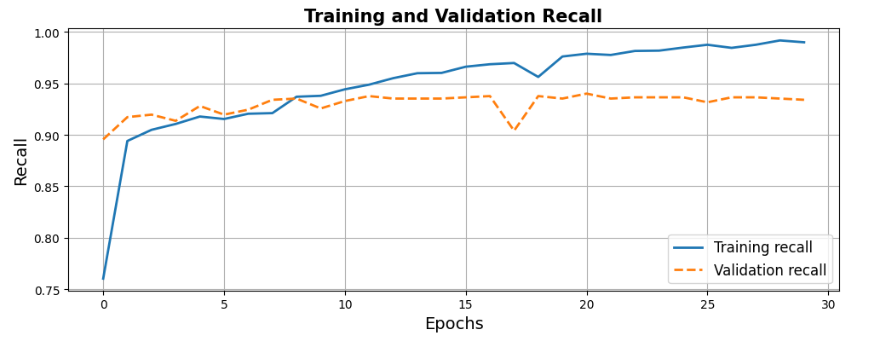


Figure - Graph of Recall

A recall graph tracks the recall metric of a machine learning model during training, plotting values against the number of epochs. Recall measures the model's ability to capture all relevant instances among actual positives. Monitoring this graph aids in optimizing the model's performance, particularly in scenarios prioritizing comprehensive identification of positive instances. It is a crucial tool in refining and evaluating classification models.

### *Graphs for F1score*

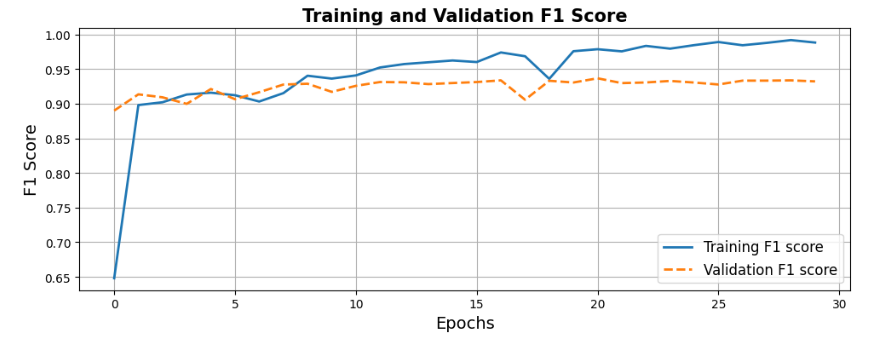


Figure - Graph of F1 Score

An F1 score graph tracks the F1 score metric of a machine learning model during training, plotting values against epochs. The F1 score, a balanced measure of precision and recall, helps monitor and optimize the model's overall classification performance. It is a key evaluation tool in refining classification models.

### *Graphs for ROC*

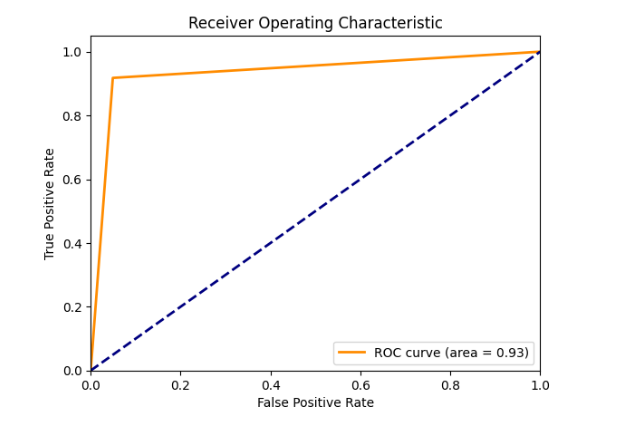
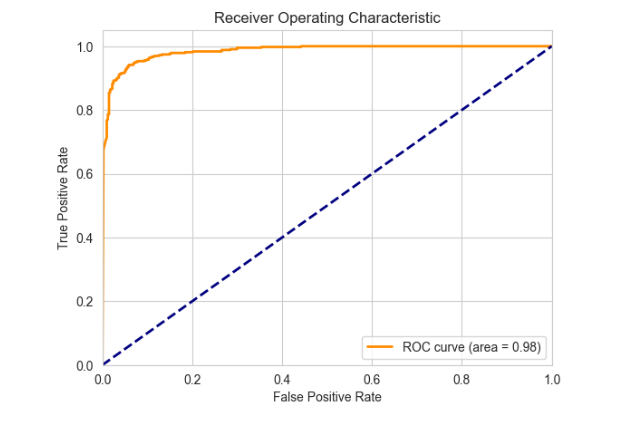


Figure - Graph for ROC

An ROC curve graph illustrates a machine learning model's ability to discriminate between classes by showing the trade-off between true positive and false positive rates across various discrimination thresholds. A higher area under the curve (AUC) indicates better overall performance. This graph is a crucial tool for assessing and comparing classification models based on their discriminatory power.



### *Confusion matrix*

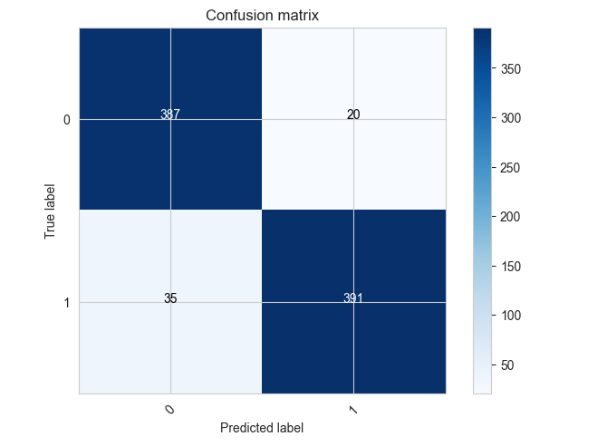


Figure - Confusion Matric

A confusion matrix graph visually summarizes the classification performance of a machine learning model by displaying counts of true positives, true negatives, false positives, and false negatives. This matrix is a crucial diagnostic tool, offering insights into the model's accuracy, precision, and recall for each class, facilitating the refinement of classification algorithms.

### Results comparison between different techniques



# CHAPTER FIVE: DISCUSSION

In this advanced strategy of Copy-Move forgeries, two methods are employed to achieve a more effective hybrid approach compared to previous techniques. Both supervised and unsupervised methodologies are employed to accomplish this objective.

Unsupervised learning constitutes a core domain of machine learning, wherein the primary objective is to investigate and discern concealed patterns and structures inherent in datasets. In contrast to supervised learning, unsupervised learning functions without the presence of explicit labels or target values associated with individual data points. The primary objectives in unsupervised learning encompass several key tasks. These tasks involve clustering, which entails the grouping of similar data points together. Another important task is dimensionality reduction, which involves the reduction of variables while preserving crucial information. Additionally, density estimation is a task that involves estimating the probability density function of data. Anomaly detection is another significant task, which involves identifying data points that exhibit substantial deviations from the norm. Lastly, generative modelling is a task that involves the creation of models capable of generating new data that closely resembles the original dataset. Unsupervised learning is extensively employed across several disciplines, including data analysis, natural language processing, computer vision, recommendation systems, and other related fields.

The supervised technique in machine learning involves training algorithms using labelled datasets, where each data point is paired with a predefined target or label. The procedure entails instructing the algorithm to generate predictions or classifications by using input features and their accompanying labels. Supervised learning encompasses several essential stages, namely data preprocessing, model construction employing diverse algorithms and approaches, prediction or inference, model assessment utilising metrics such as accuracy, precision, recall, F1-score, and potential iterative refinement in cases where the model's performance falls short of expectations. Supervised learning is frequently employed in several applications, such as picture categorization and spam email detection, among others.

Furthermore, the text alludes to the utilisation of these methodologies in the context of detecting instances of Copy-Move fraud. This assignment involves the use of four prominent algorithms, namely SURF, SIFT, Agglomerative Clustering, and RANSAC. Each of these algorithms plays a crucial part in augmenting the precision and efficacy of the forgery detection procedure.

The supervised approach employs a Convolutional Neural Network (CNN) architecture, comprising convolutional layers, batch normalisation, max-pooling, flatten and fully connected layers, output layers with softmax activation, and hyperparameter configurations. The training process employs the Adam optimizer and the Binary Cross-Entropy loss function. The model's performance is assessed by many metrics, including precision, recall, F1-score, and accuracy. The Receiver Operating Characteristic (ROC) curve and confusion matrix are commonly employed for the purpose of evaluation.

In general, the article presents a comprehensive examination of unsupervised and supervised learning methodologies, along with their utilisation in a particular issue domain. It emphasises the use of machine learning techniques for the purpose of detecting image counterfeiting.

# CHAPTER SIX: CONCLUSION AND FUTURE WORK

The technique provided for Copy-Move forgery detection, which integrates unsupervised and supervised approaches, provides a robust basis for further progress in this domain. Future research can investigate various potential avenues to improve the performance and capabilities of forgery detection systems. One potential area for investigation entails conducting further research on advanced deep learning architectures, such as convolutional neural networks (CNNs) with increased depth or cutting-edge transformer-based models. These models have the potential to capture more detailed features within images. The utilisation of transfer learning enables the refinement of pre-trained models on extensive datasets, resulting in a substantial enhancement of performance in scenarios where the availability of labelled data is restricted. Furthermore, the incorporation of a wide range of data augmentation techniques into the dataset could enhance the model's resilience against different forms of falsification.

The integration of unsupervised and supervised techniques in hybrid systems has the potential to enhance the accuracy and effectiveness of forgery detection methods. Unsupervised methodologies possess the capability to initially identify probable regions that have been forged or are of interest, but supervised models provide a more accurate means of categorization and verification. Ensemble methods, which involve the integration of predictions from several models encompassing both unsupervised and supervised techniques, have the potential to augment accuracy and robustness.

Future endeavours should also prioritise the acquisition of more extensive and varied datasets that are especially designed for the purpose of detecting instances of Copy-Move forgery. The utilisation of these datasets has the potential to enhance model generalisation and performance. Furthermore, the optimisation of models for the purpose of real-time counterfeit detection in photos or videos holds significant importance in many applications such as video content verification and live streaming. The need of interpretability and explainability is particularly pronounced within forensic domains. The establishment of methodologies aimed at elucidating the rationale behind the decisions made by a model is of utmost importance in fostering trust and comprehending the outcomes it produces. Investigating the susceptibility of forgery detection algorithms to adversarial attacks and devising techniques to enhance their resistance represents a significant domain of study. Moreover, the incorporation of forgery detection technology into the preexisting digital forensic tools utilised by professionals has the potential to augment its usefulness and accessibility.

In addition, it is crucial to consider the legal and ethical dimensions, including privacy, data protection, and compliance with legal regulations, as of utmost importance throughout the implementation of forgery detection systems. The accessibility of forgery detection can be expanded to a wider range of users by the implementation of user-friendly interfaces and technologies.

In conclusion, the constant evaluation, benchmarking against evolving forgery strategies, and expansion of forgery detection to various modalities like as audio, video, and text, will guarantee the pertinence and efficacy of these systems within a dynamic digital environment.

# REFERENCES

[1] Y. Ke, Q. Zhang, W. Min, and S. Zhang, “Detecting Image Forgery Based on Noise Estimation,”, vol. 9, no. 1, pp. 325–336, 2014

[2] Shivakumar. B. and Baboo.S, “Detection of RegionDuplication Forgery in Digital Images Using SURF,”International Journal of Computer Science Issues , vol. 8, no.4, pp. 199–205, 2011.

[3] J. Fan, T. Chen, and J. Cao, “Image tampering detection using noise histogram features,” International. Conference on Digit. Signal Process DSP, vol. 2015-September, pp. 1044–1048, 2015.

[4] J. Zhao and W. Zhao, “Passive Forensics for Region Duplication Image Forgery Based on Harris Feature Pointsand Local Binary Patterns,” Mathematical. Problems in Engineering, vol. 2013, pp. 1–12, 2013.

[5] S. Farooq, M. H. Yousaf, and F. Hussain, “A generic passive image forgery detection scheme using local binary pattern with rich models,” Computer and Electrical Engineering, vol. 62, pp. 459–472, 2017

[6] R. Dixit, R. Naskar and S. Mishra,.”Blur-invariant copymove forgery detection technique with improved detection accuracy utilising SSVD”, in IET Image Processing, vol. 11, no. 5, pp. 301-309, 2017.

[7] Zandi, M.; Mahmoudi-Aznaveh, A.; Talebpour, A. “Iterative copy-move forgery detection based on a new interest point

detector”. IEEE Transactions on Information Forensics & Security. 11, 2499–2512, 2016.

[8] X. Wang, G. He, C. Tang, Y. Han, and S. Wang, “Keypoints-Based Image Passive Forensics Method for Copy-Move Attacks,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 30, no. 3, 2016.

[9] G. Ulutas and G. Muzaffer, “A New Copy Move Forgery Detection Method Resistant to Object Removal with Uniform Background Forgery,” Mathematical. Problems in. Engineering, vol. 2016.

[10] Yang, B.; Sun, X.; Guo, H.; Xia, Z.; Chen, X. “A copy-move forgery detection method based on CMFD-SIFT”. Multimedia Tools Applications 77,pp. 837–855, 2018.

[11] D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient densefield copymove forgery detection,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2284–2297, 2015.

[12] D. G. Lowe, “Distinctive image features from scale-invariant keypoints,” Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.

[13] H. Bay, A. Ess, T. Tuytelaars, and L. C. Gool, “Speeded-up robust features (SURF),” Comput. Vis. Image Understand., vol. 110, no. 3, pp 346–359, Jun. 2008.

[14] Mikolajczyk, K., Schmid, C.,” Indexing based on scale invariant interest points”. In: ICCV. vol.1, pp. 525 – 531, 2001

[15] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT based forensic method for copy–move attack detection and transformation recovery,” IEEE TIFS, vol. 6, no. 3, 2011.

[16] R. I. Hartley and A. Zisserman, Multiple View Geometry in Computer Vision. Cambridge, U.K.: Cambridge University Press, 2004.

[17] M. Fischler and R. Bolles, “Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography,” Communication. ACM, vol. 24, no. 6, pp. 381–395, 1981.

[18] I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo, D. Tongo, G. Serra, “Copy-move forgery detection and localization by means of robust clustering with Jlinkage”. Signal Process. Image Communication 28(6), pp. 659–669,2013

[19] E. Silva, T. Carvalho, A. Ferreira, A. Rocha, “Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes”. Journal of Visual Communication and Image Representation. 29, pp. 16–32,2015

[20] C.M. Pun, X.C. Yuan, X.L. Bi, “Image forgery detection using adaptive over segmentation and feature points matching”. IEEE Transactions on Information Forensics and Security 10(8), pp.1705–1716, 2015

[21] J. Li, X. Li, B. Yang, X. Sun, “Segmentation-based image copy-move forgery detection scheme”. IEEE Transactions on Information Forensics and Security. 10(3), pp.507–518, 2015.

[22] Huang, Hui-Yu & Ciou, Ai-Jhen, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation”, EURASIP Journal on Image and Video Processing. 2019.

[23] D. Cozzolino, G. Poggi, and L. Verdoliva, “Efficient densefiel copymove forgery detection,” IEEE Transaction on Information Forensics and Security, vol. 10, no. 11, pp. 2284–2297, 2015.

[24] Raju, P.M., Nair, M.S.: “Copy-move forgery detection using binary discriminant features”. Journal of King Saud