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



**SYNOPSIS**

**FACULTY OF INFORMATION TECHNOLOGY**

**UNIVERSITY OF CENTRAL PUNJAB**

**Student Name: Hamad Malik**

**Reg -ID: L1F19MSCS0020**

**E-mail: l1f19mscs0020@ucp.edu.pk**

**Supervisor: Dr. Amjad Iqbal**

**E-mail:** [**amjad.iqbal@ucp.edu.pk**](mailto:amjad.iqbal@ucp.edu.pk)

# Abstract

In the current era, the most sorted and efficient for evidence or proof are digital images that are useful in many areas. As the internet is available for everyone at a very low cost all the users transfer a huge number of images using the internet on different social media platforms. With the increased use of smartphones in recent years, images are taken and shared on a regular basis on the internet. There are many image editing tools that are easy to use, are available openly on the internet. People use them easily to temper the image and deliver a wrong message or manipulate the evidence. This type of tempered image delivers an improper message and can influence people's life and events. Especially when our daily life or society-based matters are depending on these types of images and decisions are made on the basis of that. For example, in forensic analysis, the court of law, crime scene investigation, and so on. Due to all these concerns which the authenticity and intactness of the image is a big question. There are many tempering attacks that are done in recent times but CopyaaMoveaaforgeryaaisaathe most common. In copy-move forgery, the addition or removal of important objects from an image is done. In the past, many researchers have done work on Copy-Move Forgery-Detection. There are many CopyaaMoveaaForgery methods based on Feature-base that are made to detect the tempering attacks which is based on Blocked based and Key-point Extraction, but the results show that they are not robust in the extraction of all the features. Hence making a method to extract all the tempering regions to gain maximum results is very important. This thesis is going to overcome all the drawbacks of the past to get an optimum solution. We are going to use Key-Point Extraction with Hybrid Feature Extraction method with Hierarchical Clustering for Copy-Move Forgery Detection. Key-points are detected using SIFT-base detector and descriptor using SURF. The prior result shows an accuracy of 92.5%. We aim to get more accuracy by using our new novel approach and making it more robust.

Contents

[Introduction 3](#_Toc87548076)

[Literature Review 4](#_Toc87548077)

[Research gap 7](#_Toc87548078)

[Aim and Objectives 7](#_Toc87548079)

[Methodology 7](#_Toc87548080)

[Work Plan 8](#_Toc87548081)

[References 9](#_Toc87548082)

# 

# Introduction

We are living in the most advanced and prime era of technology where everything is depending upon technology, including our likes and daily work. The Internet is the most common part of our daily life which connects us to people and keeps us updated about the world and everything new. Social media is a part of people's lives that they use on a daily basis and share a huge number of digital images and videos on platforms like Facebook, Instagram, or Twitter. People like to share their personal life and interesting adventures on the internet through pictures or videos. Instead of all the advancements of the technologies and the social media platform still, the multi-media is the key source of getting information. Nowadays images are just not only to share about our lifestyle, but it plays a big role in sensitive matters like in a court of law, the evidence against crime, or in some research base purpose like satellite image processing, specific object tracking, or detection of specific area and programmetry.

As we talk about the internet and its wide usage and its users. There are many online tools are available that are free to use and access to any person so they can use them to edit or make some changes in an image like adding or removing the object or important information from the image. Due to this the originality and authenticity of the picture is a question for us. Living in a technological society these types of tempering can affect the society or a particular group of people. It may convey wrong information that can make people's life interesting and at the same time can make a threat to other fields. Adobe Photoshop and other powerful online tools made it very easy for us to make changes for just the sake of interest or some personal gain.

There is a multiple-way of manipulating the images like CopyaaMoveaaforgery and SplicingaaForgery. One of the passive forgery is the Copy-Move Forgery where the part of an original image is copied and then placed within the same original image. Whereas in splicing forgery the huge chunk of images come from another image. Many different post-image processing operations are used such as rescaling, affine transformation, resizing and blurring can be applied to that region which makes it more difficult to detect the change. Copy and Paste are actually not enough to create the actual forgery, many different methods have been performed to gain the tempering and fulfill the requirement. If someone wants to change the element with water or sand by overlapping the text it is difficult to detect because before pasting it in the image it is restored, resized, flipping, and blurring the tempered area to do the tempering.

A well-known Forgery type is Copy-Move Forgery where both the original and tempered region have the same comparable feature sets like pattern, shading, color schema, noise, shading components contrast, and so on. That’s why instead of being well know forging technique and working on this it is still the most difficult task to detect the tempering in it.

Manyaadifferentaaapproachesaahaveaabeenaaproposedaain theaapast that ensure the originality of image by using different algorithms and techniques. Digital signature and water marking are one of the methods. Copy-move forgery detection is also done by using the key-points that are detected by the SIFT-based descriptor. Block-based methods are also developed to use for tempering which is done by computing the similarity between the blocks to detect the text base tempering like water or sand. Discrete cosine transformation is also made to detect the overlapping text by using blocks. And many other methods are made to detect the forgery and to increase the performance of the system.

Although with all advancements and technical robustness of the system is not yet highly optimized. Yet there are many gaps and problems that are yet to be discussed and researched. The key-point-based copy-move is originally proposed by. The motivation behind this robustness is to gain more accuracy than the already existing high precision value. The novel variation to gain our goal is to use Key-Point Extraction with Hybrid Feature Extraction method with Hierarchical Clustering foraaCopyaaMoveaaForgeryaaDetection method to makeaathe system robustaaand ensureaathe originality the image by detecting the tempering region inaaimage.

# Literature Review

Several researchers have worked on the robustness of the system to gain the maximum precision of the system, proposing multiple workarounds. One of the well-known forgeries isaaCopyaaMoveaaforgeryaainaawhich bothaathe forgedaaand the original part of the image is present within the same image. Both original and tempered regions have characteristics like the same pattern, shading, noise addition, and color combination. Manyaamethodsaahaveaabeenaaproposed thataaareaaeitheraablock oraaCopyaaMoveaaForgeryaadetectionaausing Key-point based extraction. Block-based strategies [4] differentiate the given image into a block set of an overlapping element or non-overlapping element. For every block first, all the feature vector is extracted and matching is done on the similarity index. Key-point-based-detection of forgery is also very common in which the key-points sets detection, descriptions, and matching been done. SIFT is used to enhance the model. Further present [4] the J linkage algorithm and many other algorithms to make the system more robust to get an accurate result. While is this paper researcher approach an efficient detection of key-points using the approach of hybrid feature extraction method by utilizing SURF(Speed Up Robust Feature) and the SIFT detector. Then for feature matching the hierarchical clustering method is used. The results show an accuracy of 92.5% that is just not sufficient for the robustness of the machine so there is room for more enhancement of the system.

Hui-Yu Huang[6] has proposed a method for key-point-based image forgery by using Helmert transformation and Superpixel segmentation using the SLIC algorithm. The Superpixel segmentation technique gathers the pixels of photographs into the intuitive meaningful atomic shape which is used to change the pixel grid atomic region. K-Mean is used to group and generate superpixels because it adheres to the boundaries very well. For color region detection the SLIC algorithm is used. It adapts the K-men clustering to obtain the superpixels. It will cluster with the neighbor on the basis of distance to minimize the probability of seeding super-pixel with the noise pixel or with an edge. In order to make the SLIC algorithm more robust, we will minimize the size of the search area of the traditional K-mean clustering method. Helmert's transformation [6] came into work from one coordinate of the rectangle to another one so that all the points lie in the same plane. Helmert's transformation has limitations to convert different points into one point. For this reason, the affine transformation proved handy that use map coordinate transformation. The advantage of Helmert transformation is just not to stop the rotation, but it reduces the computational complexity of the system. But there is a big issue in that technique that it is highly robust against many kinds of forgeries like geometric transformation and JPGE, but it is not robust against the smooth, balanced, or constant region.

The author [7] summed up by discussing the point where the location and extraction on an image is not a problem but the issue is to detect the non-key area where the text is almost the uniform as the original text [8]. This is hard to detect the problem using a feature-based CMFD scheme. For the clarification of this problem, two new methods are proposed the notable methods [9,10]. In different scales, the SIFT feature is detectable by using scale-space representation, which is implemented on the image pyramid, and it is obtained by smoothing using Gaussian and sub-sampling of image resolution when the local extrema are selected by key-point in scale-space. Since the text is covered by the shone table is uniformed which results in only a few detection of key-points that are located. Therefore the copy-move forgery detection reach its limit and this novel approach came in handy. By using our approach the duplicate region of affine transformation is detected, but not against a region that undergoes a non-affine transformation.

Preliminary work done on the Copyaamoveaaforgeryaadetection isaabased entirely on SIFT features that are explained in the [12]. But the geometric transformation and real-time evaluation of performance are not provided. Although another author proposed the work [13]to extract the region by restoring to a correlation map, but unable to handle affine transformation and for the quantitative result onaatheaareliabilityaaofaaestimate parameters ofaageometricaatransformationaaare notaagiven. The approach [11] used to cater to the problem by SIFT algorithm which detects whether the region of an image is copy-move or not with the help of geometrical transformation. The forged region or is exact the same as the image so the key-point extraction will not be enough so SIFT algorithm be adopted to determine the possible forgery. The first step in this proposed method is the extraction of SIFT features and key-point extraction. For the second step clustering of key-point matching is done, while the third one is the estimation of geometric transformation in forgery detected.

This thesis [14] explores the work on the detection of copyaamove region inaatheaasameaaimage is detected using AKAZE features. For that merely purpose the descriptor is extracted by Modified local of different binary from key-points that are extracted from AKAZE of the image. Then the RandomaaSampleaaConsensusaaalgorithmaawasaaused to distinguish between original and false match key-points to eliminate them. The experimental results yield better results against the rotation of image, blurring the area, noiseaaaddition, andaaJPGE compressionaaattacksaacompared to similar work [15-17]. The important factor is to detect “Object Removal with uniform Background forgery” having better accuracy as compared to other work. This work [14] advantage us for non-linear scale-space creation.

To deal with the above-mentioned problem, a new concept is suggested to ensure the robustness of the system. Technically speaking, it adheres to detect the image forgery more precisely and it will boost the system and decrease the complexity and computational cost of the system. The issue that we discussed above like robustness of the system, forgeryaainaathe smooth, symmetrical, recurringaaregion, aaandaadetection of forgery onaathe non-affine transformation region. We will try to cater to all the drawbacks stated by different authors that will be solved in this new approach and make the system more robust and increase the precision of the system.

# Research gap

The robustness of the system is still an issue these days. There have been multiple studies regarding Copy-move forgery, but that varies from model to model, but they are not fully optimized. Multiple researchers try to gain the optimum robustness, but they lack to and have issues with their proposed models. The robustness of the system is still a hoax and is yet to be achieved. The maximum precision of the system is calculated and the gain is 92.5%. Moreover, the detection of copy-move forgery is common but there is yet to be research on the smooth, symmetrical, and recurring region. Researchers have been successful t detecting the tempering on the image that is in the affine transformation region, but for the detection of the image that is in non-affine transformation, the region is still an issue. The goal would be to improve this further and do adversarial training of the model to make the model robust against adversarial attacks.

# Aim and Objectives

1. This aims to improve the robustness of the system to achieve optimum precision by using Hybrid Feature Extraction.
2. This work will use techniques/ algorithms that will result in better forgery detection as compared to previous work.
3. Experiments will be performed on the MICC-F220 dataset.

# Methodology

For the robustness of the system to detect forged regions wither better results, a new architecture is needed.

1. Dividing the image
2. The process will be to divide the image into equal size patches. Because of the possibility of retouching operation and saving in a lossy compressed format, the copy-move parts may not match exactly.
3. Key-points detection by using SURF and Descriptor using SIFT.
4. Key point matching using hierarchical clustering.

Figure Flow chart of proposed Work

# 

# Work Plan



Figure Work Plan

# 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