IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Hybridization of Robust Features for Identification of Copy Move Forgery

[1]Dr G Sunil Kumar, [2]V Surya Likhitha, [3]V Ranga Reddy , [4]Shaik Ayub , [5]P Anil Kumar

[1]1Associate Professor, [2] Student (20981A04M2), [3] Student (20981A04M5), [3] Student (20981A04J6), [1]1Assistant Professor
[1,2,3,4] Electronics & Communications Engineering,
[1,2,3,4] Raghu Engineering College(A), Vishakhapatnam , India
[5] Lendi Institute of Engineering & Technology (A), Vizianagaram, India

Abstract : Nowadays, digital crime is growing at a rate that far surpasses defensive measures. Sometimes a digital media content such as an image or a video, maybe found to be in controvertible evidence of a crime or of a malevolent action. By looking at a digital data as a digital clue, multimedia forensics technologies are introducing a novel methodology for supporting clue analysis and providing an aid for making a decision on a crime. Verifying the authenticity of a digital image has been challenging problem. The simplest of the image tampering tricks is the copy-move forgery. In copy-move forgery copied portion of the image is pasted on another part of the same image. This project proposes an efficient Identification of Copy Move Forgery (ICMF) method via clustering SIFT keypoints and HARRIS corner points and searching the similar neighborhoods to locate tampered regions. In the proposed method, the keypoints are clustered based on scale and color, grouped into several smaller clusters and matched separately, which reduce the high time complexity caused in matching caused by the high dimensionality of SIFT. In order to locate the tampered regions accurately at pixel level finally, a novel localization algorithm is designed to compare the similar neighborhoods of matching pairs by two similarity measures, and mark the tampered regions in pixels iteratively. The experimental results show that the proposed method is superior to existing state-of-art methods in terms of matching time complexity, detection reliability and forgery location accuracy**.**

IndexTerms **- Copy-move forgery detection, digital image forensics, key point clustering, similar neighborhood search algorithm..**

INTRODUCTION

The digital age has transformed image creation and distribution. However, the ease of modification has made forgery possible. A common technique for forgeries is to duplicate a portion of a picture and paste it somewhere else. This can be used to alter a scene, remove undesired items, or even generate wholly manufactured images. When these manipulated photographs are utilized in court evidence, newspapers, or academic studies, the social credibility crisis will be exacerbated. As a result, image forgery detection is important. The forged picture leaves some clues which can be used to locate the manipulated regions. There are various forms of tampering procedures, and copy-move is one of the most popular. The copy-move forgery involves copying a region and pasting it into a different location in the same image and tampering an image means either adding or removing some information from an image, so that the original meaning will be changed. Copy-move forgery involves copying and pasting image portions onto the same image in order to conceal or increase some significant content in the original image. Because replicated sections appear to be identical with compatible components (such as color and noise), distinguishing between tempered and legitimate regions becomes difficult. Furthermore, a counterfeiter uses postprocessing processes such as blurring, edge smoothing, and noise to remove the visual indications of picture forgery. They initially introduced the copy-move forgery detection (CMFD) approach, which uses Discrete Cosine Transform (DCT) coefficients, and then used dictionary sorting to match the results [1]. At present, there are two popular types of copy-move forgery detection techniques: block-based and interest-based. But the block-based technique cannot withstand affine transformation attacks, and the interest point-based algorithm can only find the tampered region with limited accuracy by Fang Mei et al. [5]. A typical copy move forgery example is shown in figure 1. It is urgent to propose effective copy-move forgery detection methods to detect and locate the tampered regions for digital images.

Figure 1. Example of image forgery: original image(left) and tampered image (right).

It has been observed that the developed technique has a high success rate in detecting professional forgeries where the copied region is selected in a free-form, making it nearly impossible to detect with the human eye. Furthermore, the technique can produce successful results even when the image is subjected to postprocessing like Gaussian filtering and JPEG compression, which impede the detection of forgeries [2]. Due to the complexity of available editing tools and techniques, detecting copy-move forgery presents several challenges. These include different degrees of rotation, scaling, and noise addition applied to copied regions, as well as attempts to seamlessly blend copied areas into the background.

Researchers and practitioners use a variety of methodologies to detect copy move forgeries. These include traditional techniques like block-based matching algorithms, which compare local image patches to detect duplicated regions. Furthermore, advanced methods based on keypoint detection, such as Scale-Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF), are used to detect and match distinct features in images, providing robustness against various manipulations. The detection of copy-move forgery has thus emerged as a crucial area of research within the field of digital image forensics. By developing robust algorithms and methodologies to identify instances of tampering, researchers and practitioners seek to safeguard the integrity of digital images and uphold trust in visual media.

The remainder of the paper covers the following ,a brief introduction of the CMFD methods, an overview about SIFT features is, the method framework is described and its details are introduced briefly. Finally, the conclusion and references are provided at the end.

NEED & MOTIVATION OF THE STUDY

Digital Content Authenticity, Technological Challenges, Cybersecurity and Privacy Concerns, Scientific and Academic Contribution and Industry Applications are the needs, and the motivation to this study are Combating Digital Forgery, Technological Advancement, Ethical Responsibility, Educational and Skill Development, and Global Relevance and Impact. By addressing these needs and motivations, research in copy-move forgery detection aims to enhance the reliability and trustworthiness of digital images, protect individuals and organizations from fraud, and contribute to the scientific community with innovative solutions.

RELATED WORK.

This section discusses the research status and describes the methods used in CMFD. Copy-move forgery detection (CMFD) uses a variety of techniques to detect manipulations in which a region of an image is copied and pasted onto another part of the same image. Here's a breakdown of the two main types of CMFD methods. 1. Block-based method. 2. Key point-based method.

Block-based methods are fundamental to CMFD. They operate by dividing the image into small, overlapping or non-overlapping blocks and analyzing the features within those blocks to identify potential copy-move regions. The block-based approach to copy-move forgery detection strikes a balance between computational efficiency and detection accuracy. It detects copy-move forgeries efficiently while remaining robust to various image manipulations and transformations by dividing the image into blocks and analyzing features within these blocks. Yu Sun et al. [3] used nonoverlapping blocks as candidates in smooth regions, rather than using all the overlapping blocks. As a kind of preprocessing, grouping blocks of the same color together can be considered. First, we register the candidate blocks and then project them into hash space to prevent mismatching caused by misalignment. Block-based methods show that a suspicious image is divided into overlapped and fixed-size blocks. The tampered regions can be identified by comparing the similar feature vectors extracted from each block. Fridrich et al. [4] proposed a block-based detection scheme using quantized discrete cosine transform (DCT) coefficients, which is one of the landmark methods for detecting copy-move forgery. Babak and Stanislav et al. [6] presented a copy-move forgery detection scheme that uses blur moment invariants to extract image features from overlapped blocks. Feng Xu et al. [7] used a feature-driven prior model that relies on image features, and introduces a block-based maximum a posteriori (MAP) framework in which the image is divided into several blocks to perform SRR. As a result, the image's local features can be better characterized, resulting in a higher SRR. When recombining super resolution blocks, we still design a border-expansion strategy to remove a byproduct, namely cross artifacts. Hazizah Mohd Ijam et al. [8] developed a 2-point block backward difference method (2PBBD) for directly solving a system of nonstiff higher-order ordinary differential equations (ODEs). The method calculates approximate solutions for two points within an equidistant block at the same time. The method's integration coefficients are obtained only once, at the beginning of the integration. Numerical results are presented to compare the performance of the method developed using the 1-point backward difference (1PBD) and 2-point block divided difference (2PBDD) methods. The results showed that this method outperforms the other two methods (1PBD and 2PBDD) for finer step sizes.

As demonstrated above, most block-based methods are subject to geometric transformation attacks and have a large number of features, resulting in high time complexity. Despite these drawbacks, the block-based technique is still a useful tool for detecting copy-move forgeries, especially when combined with other complementary approaches to improve detection accuracy and reliability. Therefore, keypoint-based methods are proposed. Keypoint-based methods are techniques used to identify distinctive points or features within an image that are robust to common image processing operations such as copying, pasting, or moving regions. Keypoint-based methods offer an efficient way to detect such forgeries by analyzing specific features within the image. The first step is to identify key points or areas of interest in the image. These keypoints are image locations that stand out and

remain stable under various transformations such as rotation, scaling, and illumination changes. Keypoint detectors include SIFT (Scale-Invariant Feature Transform), SURF (Speeded-Up Robust Features), and ORB (Oriented FAST and Rotated BRIEF).
In [10] Copy move forgery involves copying a specific area and then pasting it into another region of the image. With the availability of sophisticated image processing tools, it is becoming increasingly difficult to detect forgery with the naked eye. There are rarely any visual clues to be found in the forged region of an image. To make tampering more robust, various transformations such as scaling, rotation, illumination changes, JPEG compression, noise addition, gamma correction, and blurring are used. As a result, there is a need for a method that can perform well in the face of all such attacks. This paper describes a detection method based on SURF and HAC. SURF detects keypoints and their associated features. Zhaojun Ye et al. [9] proposed the matching algorithm combines the scale-invariant feature transform (SIFT) and random sample consensus (RANSAC) algorithms to connect two images using SIFT features. To achieve a better connection, this paper improved the SIFT and RANSAC algorithms, yielding a more accurate transformation matrix between the template and scene images. The proposed grasp detection algorithm predicts multiple grasp rectangles with corresponding quality scores for objects with occlusions. Mingfu Xue et al. [11] used a novel image hashing algorithm (SSL) that incorporates the most stable keypoints and local region features and is robust to various content-preserving manipulations, including multiple combinatorial manipulations. To extract the most stable keypoints, the proposed algorithm combines Scale Invariant Feature Transform (SIFT) and Saliency detection. The Local binary pattern (LBP) feature extraction method is then used to generate local region features based on the keypoint data. Jun Zhu and Mingwu Ren et al. [12] proposed a novel image mosaic method based on the SIFT (Scale Invariant Feature Transform) feature of line segments, with the goal of resolving incident scaling, rotation, changes in lighting conditions, and other differences between two images in the panoramic image mosaic process. This method first detects key points using the Harris corner detection operator. Second, it creates directed line segments, describes them using the SIFT feature, and then matches those segments to obtain rough point matching. Finally, the Ransac method is used to remove incorrect pairs in order to complete the image mosaic. The results of an experiment with four pairs of images show that our method is very robust in terms of resolution, lighting, rotation, and scaling.
A copy-move forged image is the outcome of a particular kind of image tampering technique wherein an image portion is copied and pasted onto one or more other portions of the same image, usually with the intent to clone or purposefully hide undesirable regions or objects. Thus, the key task in detecting such forgeries is to come up with methods of exposing portions in photos that are identical or relatively comparable by Wandji Nanda Nathalie Diane et al. [13]. By focusing on distinctive image features, keypoint-based methods can potentially reduce false positives. Random noise or slight variations in lighting might trigger false positives in block-based methods, but keypoints are less susceptible to such inconsistencies. Keypoint-based methods offer a compelling approach for copy-move forgery detection. They provide a good balance between speed, robustness to geometric manipulations, and the ability to handle partial forgeries. This makes them a valuable tool for image forensics. Therefore, this paper is compared to the traditional method.

SIFT FEATURE.
SIFT (Scale-Invariant Feature Transform) features are widely used in copy-move forgery detection (CMFD) due to their robustness to various image transformations. SIFT features have been widely used in CMFD due to their robustness and effectiveness in detecting duplicated regions, even in the presence of various transformations and distortions. However, it's worth noting that SIFT-based approaches may be computationally intensive, especially for large images, and may not perform optimally in scenarios with significant image noise or compression artifacts.
The SIFT algorithm is designed to find keypoints (feature points) in various scale spaces and calculate their dominant orientation. SIFT identifies some very prominent points, such as corners, edges, bright spots in dark areas, and dark spots in bright areas, that are unaffected by illumination, affine transformation, or noise. The SIFT keypoints have been selected as local extrema within a 3×3×3 cube of the DOG domain. More specifically, the DoG image at scale σ is given by,

where

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (1)$$

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (2)$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (3)$$

Fitting the three-dimensional quadratic function allows you to accurately determine the position and scale of the keypoints. Within the domain of forgery detection, SIFT is a well-known and enduring feature descriptor. The SIFT algorithm's primary function is to locate keypoints, or feature points, in various size areas and determine which keypoint orientation is dominant. A few highly noticeable places, such as corners, edges, bright spots in dark areas, and dark spots in bright areas, that remain unchanged in the presence of noise, affine transformation, and lighting are the key points identified by SIFT. The primary computational steps involved in producing feature sets for images. An effective approach based on SIFT keypoints scale-color clustering and comparable neighbourhoods searching is devised, according to the conventional CMFD process. The general structure of the suggested approach. The suggested approach includes the following steps: feature extraction, feature matching, mismatch elimination, keypoint clustering, and tampering region localization. First, keypoints were described using SIFT. Next, we group the keypoints into multiple smaller clusters that have been independently matched by clustering them according to colour and scale. The affine transformation matrix is estimated and mismatches are eliminated using the J-Linkage algorithm. Lastly, altered regions are found by searching similar neighbourhoods of matched couples.

KEYPOINTS SCALE-COLOR CLUSTERING.
Given the abundance of SIFT keypoints, particularly in high-resolution photos, there are two issues with matching:1) Feature matching has an O(n2) temporal complexity, where n is the number of keypoints. In actuality, correct matching pairs account for a small share; 2) the time complexity will increase in square order as the value of n increases. While matching, every point must be compared with n-1 other points, most of which are superfluous. Thus, in order to lower the computational cost of matching, keypoints must be clustered before feature matching.

The hierarchical feature point matching approach is enhanced in this study in order to address the aforementioned issues. The scale-color clustering system based on SIFT keypoints. It's divided into two sections: 1) Clustering using overlapped scale; 2) Clustering using keypoint color.

Clustering Based On Overlapped Scale.

SIFT keypoints are extreme points in the Gaussian scale space. According to the third element σk in the descriptor, each octave of keypoints has a corresponding scale. It is rare for the scales of the two keypoints in matching pairs to be significantly different from one another, as the majority of keypoints that can be matched have comparable scales. Consequently, this step's primary goal is to maximise the distance between keypoints on various scales in order to minimise pointless matching and comparison. We keep the large-scale range and group the small-scale range together because we know there are fewer large-scale keypoints than there are small-scale keypoints. In order to preserve the resilience against scaling attack manipulation, overlapped scale is used for scale clustering concurrently.

Color-Based Clustering.

Following scale clustering, Sl and Sm will include a sizable number of low-scale keypoint clusters. To further reduce the temporal complexity, color-based clustering is used. Because the modified region and the source region are similar, even after a geometric modification or post-processing action, the associated matching points will not significantly alter in color. A certain amount of inaccuracy and redundancy may result from converting distinct RGB values to the same grey value when converting color images to grayscale. The image's visual characteristics can be preserved to the greatest extent possible because the RGB value of the keypoint in the tampered region does not significantly change. Thus, predicated upon Following the previous stage, we continued to use the color-based clustering approach, applying color clustering to the Sl, Sm, and Sh groups, respectively.

HARRIS CORNER POINTS.

Used in computer vision algorithms to extract corners and deduce visual properties, the Harris corner detector is a corner detection operator. By simply evaluating the difference in corner score with respect to direction instead than requiring shifting patches for each 45-degree angle, Harris' corner detector is more accurate in differentiating between edges and corners. Since I am the intensity value of each pixel in our 3 x 3 window and (u,v) are the (x,y) coordinates of each pixel, let's define E(u,v) as the sum of all the sum squared differences (SSD). Pixels with high E(u,v) values, as defined by a threshold, comprise the features of the image. The function E(u,v) must be maximised in order to detect corners.

The function E(u,v) must be maximised in order to detect corners.

$$E(u,v) = \sum_{x,y} w(x,y)[I(x+u, y+v) - I(x,y)]^2 \qquad (4)$$

Lastly, the copy move forged image is identified by combining the features that were retrieved using HARRIS and SIFT. After combining these QQ1 characteristics using SIFT and HARRIS, they are clustered according to colour and size, resulting in multiple smaller clusters that have been independently matched. A corner is a location where the local neighbourhood is oriented in two distinct and dominating edge directions. Put differently, a corner is the intersection of two edges, where an edge is a sharp shift in image brightness. Generally referred to as interest spots that are independent of translation, rotation, and lighting, corners are the most significant characteristics in an image. Even though they make up a small portion of the image, corners are the most crucial features for restoring image information. Because of this, they can be used to reduce the amount of processed data needed for tasks like stereo vision, image representation, motion tracking, image stitching, and other related computer vision applications. The detailed steps for Combining SIFT and Harris Features for Copy-Move Forgery Detection is depicted in the below figure 1

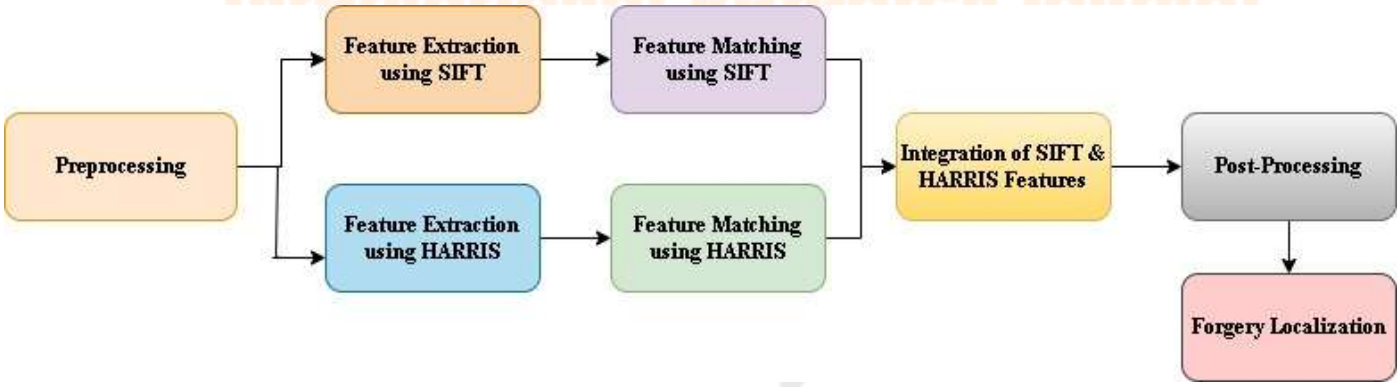

Figure 1. The framework of the proposed method

Preprocessing

1. Grayscale Conversion: Convert the input image to grayscale to simplify the processing.
2. Noise Reduction: Apply Gaussian smoothing or other denoising techniques to reduce noise, which can improve feature detection.

Feature Extraction:

a. SIFT Features: Detect keypoints and descriptors using the SIFT algorithm. SIFT is robust to scale and rotation changes.
   1. Compute the Difference of Gaussians (DoG) to find keypoints.
   2. Assign orientations to each keypoint based on local gradient directions.
   3. Generate SIFT descriptors for each keypoint.

b. Harris Corners: Detect Harris corners, which are good at finding points with significant intensity changes.
   1. Compute the gradient images I_x & I_y by convolving the grayscale image with Sobel filters.
   2. Calculate the Harris matrix for each pixel.
   3. Compute the Harris response and threshold it to find corner points.

Feature Matching:

1. SIFT Matching: Match SIFT descriptors using a nearest-neighbor approach, typically with a ratio test to filter out poor matches.
2. Harris Matching: Match Harris corners by comparing local neighborhoods (e.g., using normalized cross-correlation).

Combining Features:

1. Integrate SIFT and Harris features by concatenating or fusing their descriptors.
2. Alternatively, you can run SIFT and Harris independently and then combine their matched regions for a final decision.

Post-Processing:

1. Geometric Verification: Use RANSAC (Random Sample Consensus) to eliminate outliers and verify the geometric consistency of the matched regions.
2. Region Merging: Merge overlapping matched regions to form larger, coherent duplicated areas.

Forgery Localization:

1. Mark the detected duplicated regions on the image.
2. Optionally, apply morphological operations to refine the boundaries of the detected regions.

RESULTS AND DISCUSSION.

The experiments are conducted on the tampered images of a public domain benchmark databases GRIP. The GRIP database contains 2 × 80 = 160 ground truth images and tampered images which tampered regions have arbitrary shape, ranging in size from 4000 pixels (less than 1% of the image) to 50000 pixels. The average size of tampered region is about 10% of each image. Tampering means include rotation, scaling, JPEG compression and noise.

All the experiments are conducted on a machine with Intel(R) Core (TM) i3-4005U CPU @1.70GHz 4GB RAM and runs on Matlab R2018a.

The effectiveness of the suggested technique is evaluated on a micro and macro level, analyzing both the overall image quality and individual pixel precision. We examine how accurately images can be identified as fake or real, specifically looking for basic copy-and-paste forgeries. We meticulously scrutinize individual pixels to assess the method's ability to accurately identify manipulated areas, ensuring its reliability and strength. In this study, the altered images/pixels are viewed as successes while the genuine images/pixels are seen as failures, using the True Positive Rate (TPR), False Positive Rate (FPR), and F1 to assess the effectiveness of the suggested techniques. TPR showcases the percentage of manipulated images that are accurately identified in the detection outcome. They are defined as follows:

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

$$FPR = \frac{FP}{TP+FN} \quad (6)$$

$$F1 = \frac{2TP}{2TP+FP+FN} \quad (7)$$

In this context, TP (True Positive) represents the count of tampered images/tampered pixels correctly classified as tampered; FP (False Positive) signifies the count of authentic images/authentic pixels incorrectly classified as tampered; TN (True Negative) denotes the count of authentic images/authentic pixels accurately classified as authentic; and FN (False Negative) indicates the count of tampered images/tampered pixels erroneously classified as authentic.

Sl no	Input tampered Image	Forgery detection using SIFT	Forgery detection using SIFT& HARRIS
1			
2			
3			
4			
5			
6			

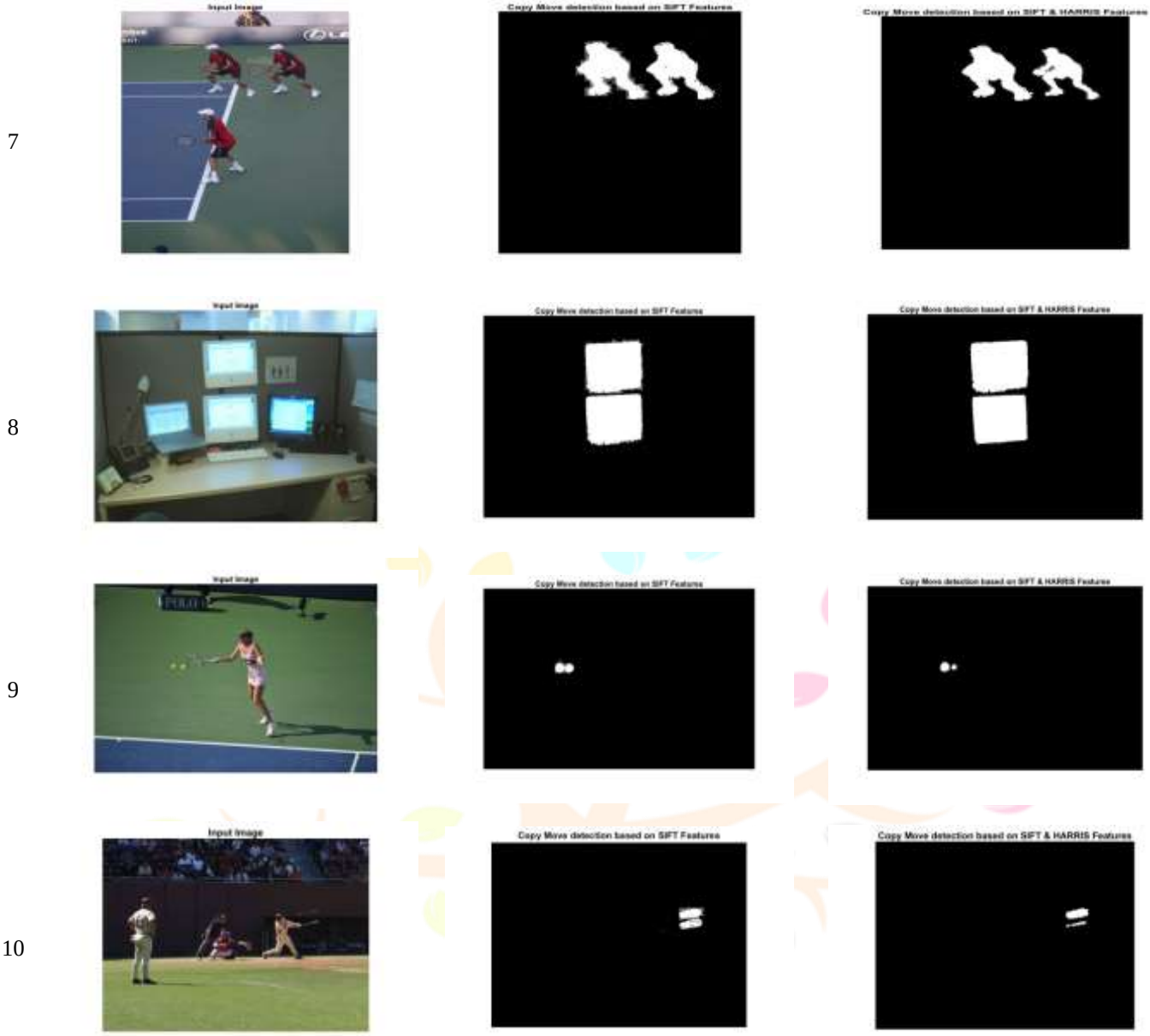

Figure 2. Comparative results: (a) tampered image, (b) experimental results with SIFT,

(c) experimental results with SIFT and HARRIS.

Figure 2 illustrates the comparative experimental results of detected tampered regions using the Proposed and SIFT techniques. Table 1gives the evaluation results of the method at image level and pixel level, and the experimental data are averaged.

Table 1. Experimental results of simple forgery in GRIP

Input	Method	TPR	FPR	F1-Imgae level	Precision	Recall	F1- Pixel level
Input 1	SIFT	90.72	10.27	90.15	99.64	99.56	99.60
	SIFT+HARRIS	91.83	8.99	91.81	99.88	99.80	99.89
Input 2	SIFT	90.49	10.05	90.18	99.48	99.71	99.59
	SIFT+HARRIS	91.76	8.12	91.82	99.84	99.84	99.84
Input 3	SIFT	90.17	9.73	90.22	99.48	99.71	99.59
	SIFT+HARRIS	92.55	8.88	91.74	99.92	99.76	99.84
Input 4	SIFT	90.36	9.92	90.20	99.52	99.67	99.59
	SIFT+HARRIS	91.87	8.23	91.81	99.96	99.72	99.84
Input 5	SIFT	90.36	9.92	90.20	99.52	99.67	99.59
	SIFT+HARRIS	91.80	8.16	91.82	99.84	99.84	99.84
Input 6	SIFT	90.52	10.08	90.18	99.52	99.67	99.59
	SIFT+HARRIS	92.27	8.62	91.77	99.80	99.87	99.83
Input 7	SIFT	89.29	8.80	90.33	99.60	99.60	99.60
	SIFT+HARRIS	91.73	8.09	91.82	99.80	99.87	99.83
Input 8	SIFT	90.07	9.63	90.23	99.56	99.63	99.59
	SIFT+HARRIS	92.07	8.42	91.79	99.84	99.84	99.84
Input 9	SIFT	89.85	9.40	90.26	99.56	99.63	99.59

	SIFT+HARRIS	91.27	7.62	91.87	99.88	99.80	99.84
Input 10	SIFT	90.95	10.49	90.13	99.48	99.71	99.59
	SIFT+HARRIS	91.80	8.16	91.82	99.80	99.87	99.83

Conclusion.

In this paper, we present a novel CMFD method based on SIFT & HARRIS keypoint to locate the doctored regions at the pixel level, and the experimental results show that the method has performed well The combined approach of SIFT and Harris techniques for copy-move forgery detection leverages the strengths of both methods to achieve higher detection accuracy and robustness. SIFT's invariance to transformations and rich descriptors, coupled with Harris's computational efficiency and corner detection, create a powerful tool for identifying duplicated regions in images. The combined method effectively reduces false positives, handles diverse image content, and provides reliable detection of copy-move forgeries, making it a valuable approach in digital image forensics.

Future Scope.

The future research on copy-move forgery detection using a combined approach of SIFT and Harris techniques is poised to make significant strides in enhancing the accuracy, efficiency, and robustness of digital forensics. By integrating advanced feature extraction methods, improving matching algorithms, and leveraging emerging technologies, researchers can develop more powerful and versatile forgery detection systems. These advancements will not only help in combating digital image manipulation but also contribute to the broader field of digital forensics and cybersecurity.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Associate Professor Dr. G Sahu ,department of ECE, REC for his invaluable guidance and insightful feedback throughout the research process. His expertise and encouragement greatly contributed to the success of this project. We appreciate the technical support provided by the department of ECE, REC for their assistance with the data processing and analysis tools. Additionally, we acknowledge the constructive comments and suggestions from the anonymous reviewers, which helped improve the quality of this paper.

Finally, we would like to express our deepest appreciation to our families and friends for their unwavering support and encouragement throughout the duration of this research.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukaiai, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Citeseer, 2003.

[2] Emre Gurbuz, Guzin Ulutas and Mustafa Ulutas. "Detection of Free-Form Copy-Move Forgery on Digital Images". Received 03 April 2019, Accepted 30 July 2019.

[3] Yu Sun, Rongrong, Yao Zhao. "Nonoverlapping Blocks Based Copy-Move Forgery Detection". Received 29 September 2017, Revised 12 December 2017, Accepted 18 December 2017.

[4] J. Fridrich, D. Soukalm, and J. Lukas, "Detection of copy-move forgery in digital images," Digital Forensic Research Workshop, pp. 19–23, 2003.

[5] Fang Mei, Tianchang Gao and Yingda Lyu. "CF Model: A Coarse-to-Fine Model Based on Two-Level Local Search for Image Copy-Move Forgery Detection". Received 10 December 2020, Revised 27 March 2021, Accepted 12 April 2021.

[6] M. Babak and S. Stanislav, "Detection of copy move forgery using a method based on blur moment invariants," IEEE Transactions on Information Forensics, vol. 10, no. 3, pp. 507–518, 2007.

[7] Feng Xu, Tanghuai Fan, Chenrong Huang, Xin Wang, Lizhong Xu, "Block-Based MAP Superresolution Using Feature-Driven Prior Model," Received 18 Oct 2013, Revised 27 Jan 2014, Accepted 29 Jan 2014, Published 18 Mar 2014.

[8] Hazizah Mohd Ijam, Mohamed Suleiman, Ahmad Fadly Nurullah Rasedee, Norazak Senu, Ali Ahmadian and Soheil Salahshour, "Solving Nonstiff Higher-Order Ordinary Differential Equations Using 2-Point Block Method Directly," Received 18 Jul 2014, Accepted 23 Aug 2014, Published 17 Sept 2014.

[9] Zhaojun Ye, Yi Guo, Chengguang Wang, Haohui Huang, and Genke Yang, "Grasp Detection under Occlusions Using SIFT Features," Received 30 Aug 2021, Accepted 22 Oct 2021, Published 13 Nov 2021.

[10] Parul Mishra, Nishchol Mishra, Sanjeev Sharma, and Ravindra Patel, "Region Duplication Forgery Detection Technique Based on SURF and HAC," Received 16 Aug 2013, Accepted 17 Sept 2013, Published 07 Nov 2013.

[11] Mingfu Xue, Chengxiang Yuan, Zhe Liu, and Jian Wang, "SSL: A Novel Image Hashing Technique Using SIFT Keypoints with Saliency Detection and LBP Feature Extraction against Combinatorial Manipulations," Received 14 Nov 2018, Revised 12 Jan 2019, Accepted 07 Feb 2019, Published 03 Mar 2019.

[12] Jun Zhu and Mingwu Ren, "Image Mosaic Method Based on SIFT Features of Line Segment," Received 26 Sept 2013, Accepted 17 Nov 2013, Published 06 Jan 2014.

[13] Wandji Nanda Nathalie Diane, Sun Xingming and Fah Kue Moise. "A Survey of Partition-Based Techniques for Copy-Move Forgery Detection". Received 02 June 2014, Accepted 06 July 2014..