Received: 22 March 2024 | *Revised:* 18 June 2024 | *Accepted:* 18 June 2024
DOI: 10.37917/ijeee.22.1.26 *Vol. 22 | Issue 1 | June 2026*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access
IJEEE University of Basrah College of Engineering

A Robust Hybrid Multi-Scale Approach to Detect Copy-Move Forgery in Digital Image

Manaf Mohammed Ali Alhaidery*, Israa Abdulkadhim Jabbar Al Ali, Noura Jumaah Ahmed Alqaysi
University of Kerbala, College of Education for Human Sciences, Kerbala, Iraq

Manaf Mohammed Ali Alhaidery
University of Kerbala, College of Education for Human Sciences
Email: manaf.m@uokerbala.edu.iq

Abstract
With the development of cyber security and multimedia forensics, digital image manipulation has recently been recognized as one of the major challenges in forensic image analysis. Therefore, selecting an image area and then copying and pasting it into the same image is the hardest process in passive image forgery. This act violates privacy and secrecy of authenticity of digital image. The attacker exploits the available tools of editing image program to make the fake image similar to the original one. This paper presents a proposed fast and efficient passive Copy-move forgery detection scheme. Hessian- Affine and Harris-Affine detectors, and Shift Invariant Feature Transform (SIFT) descriptor, are employed in the proposed scheme. These detectors provide sufficient key points for detecting the duplicated regions in the case of small or invisible regions. The experimental results show that the proposed scheme is invariant against simple and hard attacks like uniform or non-uniform transformation. The proposed scheme was evaluated using standard data sets (GRIP, MICC 220, and F8 Multi). Resulted True Positive Rate (TPR) was 0.98 and False Positive Rate (FPR) was 0.035. Thus, the scheme is effective and providing valuable results compared to recent passive image authentication schemes.

Keywords
Image Forensic, Copy-Move Forgery, Multi-Scale Approach, Harris-Affine Detector, Hessian-Affine, SIFT.

I. Introduction

Digital data is more widespread than ever due to the development in digital communication and international network. Digital images are the basic source of digital data. These are used in various fields such as E-government, military, and weather researches. Given the availability of digital images on these networks, the biggest challenge is ensuring the protection of these images. Therefore, verifying the authenticity of the image has become necessary and required [1]. Image forensic approaches aim to ensure the authenticity of digital images and preserve them from forgeries and attacks to manipulate image content. In the field of image forgery, we have passive and active approaches as shown in Fig. 1. The Passive approach consider visible one while active approach is invisible [2]. Passive approaches can be classified into three main types, copy-move, splicing, and retouching. In the active approach, there are two intermediate objects: the source image and the embedded data. The attacker embeds an electronic signature or tag in the source image. In contrast, the passive approach is universal and widely used in image forensic schemes. Cloning or copy-move forgery approach is more common than retouching or splicing approaches and it considers more complex. Where, part of target image is elicits and pasted on the other side of image. This process aims to hide or falsify the meaning of that image [3]. Different editing image programs like Photoshop, Paint are used to perform copy-move forgery process. Therefore, passive image forensic scheme is sensitive task to determine the authenticity of digital image. In this paper, we present a hybrid Copy- Move Forgery Detection (CMFD) scheme by combining Hessian-affine and Harris–affine as detectors and SIFT technique as descriptor. The reasons of selecting these detectors are firstly: increasing the quantity of features from target image. Secondly, the selected detectors have able to detect the duplicated regions from forged image under simple and complex transformations

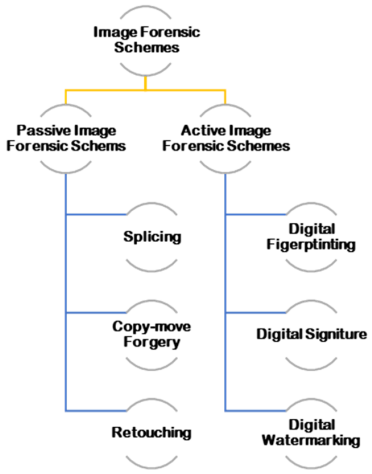


Fig. 1. Classification of Image Forensic Schemes.

like affine transformations. Thirdly, the ability of detectors to detect the homogeneous and invisible cloning regions. So, our contributions in this paper are denoted below:

- We presented a robust Multi-Scale scheme to detect the iterative regions under hard conditions like non-uniform transformations.
- In the proposed scheme we address the problem of invisible and small duplicated regions by using Hessian and Harris-Affine detectors.
- The suggested scheme can reveal and localize single and multiple duplicated regions under different conditions.
- To improve the quality of detection , Maximum Likelihood Sample Consensus Algorithm (MLESAC) is used as a false positive filter to isolate false results and support correct results.

The remainder of the paper arranges as follows. Section II. presents related works. Section III. demonstrates a proposed scheme steps. Section IV. states the evaluation metrics, dataset, results, and comparison with other schemes. Section V. clarifies the resultant and new ideas.

II. Related Work

Various proposed methods are presented in the passive CMFD framework. There are three main types approaches: The block-based approach, the keypoint-based approach and a combination of them. These schemes differ in their feature detection methodology. The procedure of these methods involve revealing and describing features of the test image, and then matching those features to find iterative patches. The first proposed method of this kind of passive image forgery detection was developed by Fridrich et al. [4] , using a block- based scheme based on Discrete Cosine Transform (DCT). Popescu and Farid [5] replaced DCT by using Principle Component Analysis (PCA) to represent the overlapping blocks then the features are elicited from each block. Different papers are adopted block-based technique like [6, 7]. In other side, The keypoint-based technique extracts features from the source image and then applies feature description to get unique descriptor vectors. These vectors are compared with each other using Euclidean distance to extract duplicate regions. Amirini used SIFT detector as keypoint- based technique in the detection stage. [8] Gani et al. used package-clustering algorithm to divide the blocks of DCT coefficient vectors, and then find matching vectors in each package [9]. Kashyap and Joshi utilized blur moment invariants and DWT by eliciting moments from each block then using PCA to improve the performance of the suggested scheme [10]. The main disadvantages of block–based technique are consuming time to detect the duplicated regions and the weakness detection under uniform geometric attacks. On the other hand, different approaches have been used parallel block-based techniques to improve the quality of image forgery detection. Some researchers used parallel feature-based techniques to improve the quality of copy-move forgery detection [11, 12] . Meanwhile, others used parallel and serial block–based techniques [13]. In contrast, several approaches have proposed a serial feature-based technique with a block-based technique to extract the positive properties of both[[14]. In our proposed scheme, parallel feature-based techniques are used. We selected excellent detectors like Harris-affine and Hessian affine [15] detectors to raise the quality of forgery detection from visible and invisible duplicated regions. Additionally, the ability to reveal the forgery regions under uniform and non-uniform transformation attacks.

III. Proposed Method

Affine transformation attacks consider the main challenge for inspection the quality performance of any image authentication scheme. Therefore,we presented a hybrid detector to enable the proposed scheme to satisfy quality in revelation and localization the duplicated regions. In this scheme, we adopted two affine detectors (Harris and Hessian) for multi logical reasons:

- To obtain sufficient key points from target image that help us to reveal until small and homogeneous iterative patches in the digital image.
- These Harris and Hessian affine detectors capable to

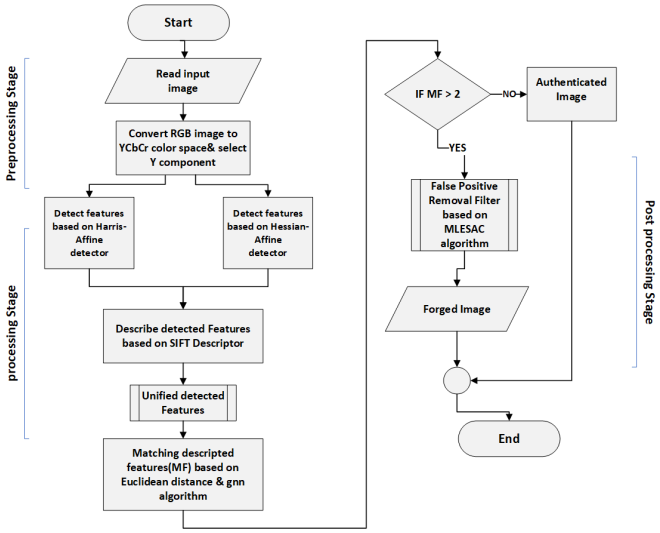
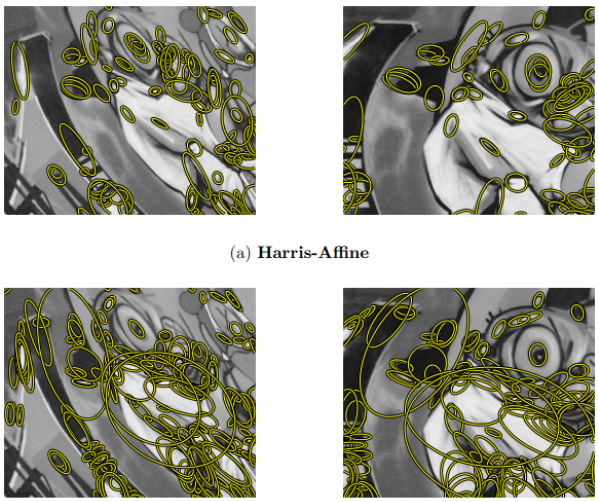


Fig. 2. The proposed CMFD scheme.



(a) **Harris-Affine**

(b) **Hessian-Affine**

Fig. 3. : Detection interest points with (a) Harris-Affine (b) Hessian affine detectors.

detect the cloning regions under hardest conditions like geometrical or affine attacks.

- The fusion of these detectors makes the proposed scheme qualified for localization the duplicated regions without any morphological processing.

Hence, Fig. 2 shows the proposed scheme that includes three main stages: pre-processing, processing, and post processing stages.

A. Prepossessing Stage

In this stage, the (RGB) Color space of digital image are converted into another one like (YCbCr) Color space [16]. The luminance or (Y) component is more important than chrominance (Cb, Cr) components because it include the majority information of digital image while the other component contain the additional details like color. Therefore, we select luminance component (Y) as input of processing stage. The conversion equation that it extracts gray scale or (Y) component is denoted below:

$$Y = 16 + \frac{65.7 * R}{256} + \frac{129.057 * G}{256} + \frac{25.064 * B}{256} \qquad (1)$$

1) Processing Stage

This stage are involves two processes, detection and description.

Detection Process

The efficiency of any key-point based detector is depending on the quality and quantity of extracted interest points from digital image. The quality refer to the ability of detector versus brightness, uniform and affine transformations while the quantity refer to the amount of interest points in small and homogeneous image regions. In this stage, we select two key point detectors to recover the data of all image content. The first one is called Hessian- Affine and another called Harris-Affine. The performance of these detectors in terms of resistance to attacks and the ability of detection were high. The repeatability of detection key points is important factor in local invariant detectors. Both of the selected detectors are able to reveal duplicated interest points under geometric, photometric attacks and affine transformations as shown in Fig. 3. The second moment matrix is used in Harris-Affine detector. The Hessian-Affine detector elicits the interest points by using the Hessian matrix :

$$H(x) = \begin{bmatrix} L_{xx}(x) & L_{xy}(x) \\ L_{yx}(x) & L_{yy}(x) \end{bmatrix} \qquad (2)$$

The interest points, which detected and localized by using iterative search technique and Laplacian of Gaussian's.

Description Process

In our scheme, we have two detectors (Harris and Hessian Affine detectors), each of which detects interest points independently. Descriptor technique is used to uniquely identify the detected points. We used SIFT technique [17] as descriptor to improve the quality of detected features in the matching stage. The detected points from both detectors are standardized or unified and then converted into feature descriptors. The output of detector-descriptor processes is high quantity of features, which cover all the areas of image in texture and homogeneous cases. This quantity of detected features supports ability of scheme to extract the duplicated regions from the target image.

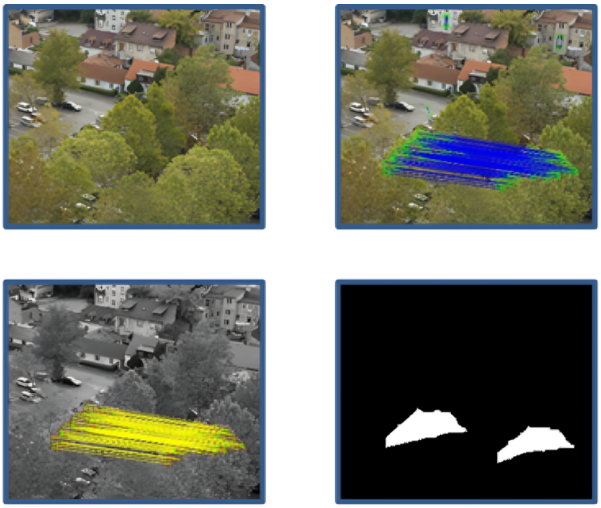


Fig. 4. First row: (a) The source image,(b) After hybrid detection, Second row: (c) After MLESAC filter, (d) localized duplicated regions.

IV. Post processing Stage

In this stage, the similar duplicated features are extracted in matching process then applying FPR filter to isolate the real duplicated features as false features.

A. Matching and Refinement Output Results

Matching the detected features to each other is important task in order to extract matching features. Euclidean distance [18] is employed as a metric of matching features where a smaller distance indicates a higher degree of similarity. The Euclidean distance between (x_1, y_1) and (x_2, y_2) points as exposed in equation below:

$$d^E(f, f') = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \tag{3}$$

After matching features, the greatest Nearest Neighbor (g2NN) algorithm is used to obtain the basic duplicated features.This algorithm compares between the distance of the first and the nearest neighbor with a threshold value (τ)

$$d_i / d_{i+1} < \tau \tag{4}$$

The results of these processes are pair of matching features as shown in Fig. 4. The matched features are classified in to True positive (TP) and False positive (FP) features. However, we examine and use different False positive removal filters as post processing stage to remove the outlier features and improve the quality of proposed scheme. These filters are:

- Random Sample Consensus filter (RANSAC) algorithm.
- Maximum Likelihood Estimation Sample Consensus (MLESAC) algorithm.

TABLE I. Datasets of CMFD

Dataset	'Auth./Forg.'	Size	Mask
GRIP	80	768*1024	Yes
MICC-F600	440/160	800*533	Yes
MICC-F8 Multi	8 multi	1995*1136	No

- Hough Transform (HT) algorithm.
- Distance Ratio algorithm.

FThe main task of these filters is excluding the false results and including the true results. The False results refer to false positive features (FP) while the True results refer to true positive features (TP).
The ability and the speed of these filters are differing under geometric and lighting attacks. Therefore, we examine all these false removal algorithms in standard dataset images. These images are changed like smooth, invisible duplicated regions with simple and hard attacks like non-uniform transformation attacks. The aim of utilizing various filters is to perform comparison between them in terms of simple and complicated attacks like affine transformation. In addition, we examined the robustness of proposed scheme in case of small and hidden duplicated regions.

V. Result and discussion

In this part, we test and evaluate the robustness of the presented method. The standard evaluation metrics are used to assess the performance and efficiency of the proposed scheme. The output image include True Positive (TP) and False Positive (FP) parts. Therefore, we used two evaluation metrics True Positive Rate (TPR) and False Positive Rate (FPR) as noted below [19].

$$TPR = \frac{TP}{TP + FN} \tag{5}$$

$$FPR = \frac{FP}{FP + TN} \tag{6}$$

The proposed method was implemented on an Intel Core i5 2.6 GHz processor and (16 GB) RAM and executed in MATLAB R2022b environment. The proposed scheme was tested on various datasets GRIP, MICC-F600, and MICC-F8 [20] as shown in Table I. The main reason for using the GRIP dataset is that it consists of binary images corresponding to fake images. These binary images are needed to evaluate the scheme using pixel-level metrics.

TABLE II. THE PERFORMANCE UNDER PHOTOMETRIC ATTACKS

	Adding noise	0.001	0.01	0.05
Photo.Attacks	TPR	100	99	98.4
	FPR	0	2	2
	Smoothing	3*3	4*4	5*5
	TPR	100	99	98
	FPR	0	1	2
	Color variation	0.1	0.01	0.15
	TPR	100	99.5	98
	FPR	0	1	2
	JPEG quality	3	7	9
	TPR	100	97.5	96
	FPR	0	3	4.5

TABLE III. THE PERFORMANCE UNDER TRANSFORMATION ATTACKS

	scaling	0.001	0.01	0.02
Transf.Attacks	TPR	100	99	97
	FPR	0	1	2
	Orientation	5 deg	20 deg	30 deg
	TPR	100	99	98
	FPR	0	1	1

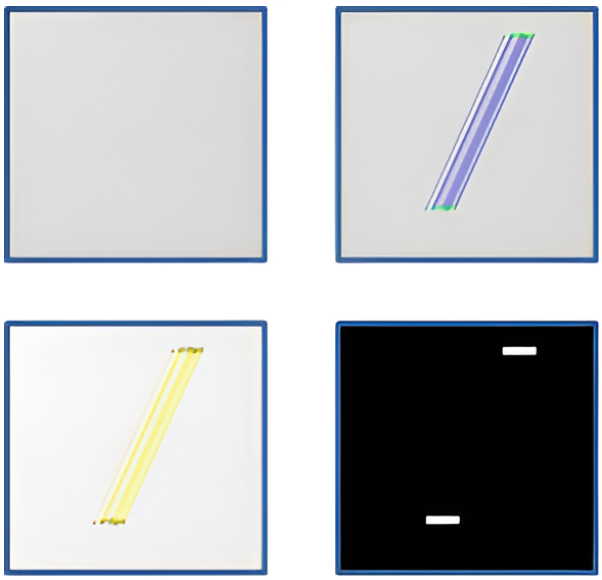


Fig. 5. Result of the proposed scheme with small and hidden duplicated regions. First row: (a) The source image,(b) After detection regions, Second row: (c) After filtering process, (d) localizing the duplicated regions.

A. Testing the proposed scheme under attacks

This section involved testing our scheme in terms of:

- Simple attacks like uniform transformation, brightness attacks.
- Complex attacks like affine transformations attacks and small, hidden duplicated regions attacks.

1) Invariance of the proposed scheme for simple photometric and geometric attacks

To investigate the quality of the scheme, we used forged images with photometric attacks such as (smoothing, noise, image color variation, JPEG quality) and geometric attacks such as (translation, scaling and orientation). We calculated the value of the evaluation metrics TPR and FPR for these attacks, as shown in the Table II, Table III and Fig. 5. The Table II shows the performance levels of scheme under photometric attacks. Table III demonstrates the value of TPR, FPR under uniform transformation attacks.

2) Invariance of the proposed scheme for small and hidden duplicated region attacks

Detection the small or hidden duplicated regions represents the critical challenge in passive image authentication scheme and most of proposed approaches failed to detect the iterative regions under these conditions.

However, the proposed scheme has the ability to detect the duplicated regions when these regions are small or hidden. We tested the performance of this scheme under hidden and small duplicated regions. The ability of our technique to detect small homogeneous and invisible duplicated regions is shown in Fig. 5. Furthermore, the suggested technique can detect hidden duplicated regions until using transformation and photometric attacks.

3) Invariance of the proposed scheme for multi hidden duplicated regions

We evaluated the suggested method with several duplicated regions and an affine transformation in the invisible source image, as shown in Fig. 6, where one duplicate was copied without modification and the other was duplicated with a (20) degree rotation and an affine transformation. The output result illustrates how well the recommended strategy performs in complex attack scenarios (invisible forged image, multi duplicated regions and affine transformation).

B. Comparison with recent CMFD schemes

In this section, different recent proposed methods are selected to make comparison process. This process give us ability to evaluate the proposed method. We compared the results with these methods by using TPR, FPR metrics. These methods are Amerini [8], Meena [21], Yıldız [16], Raju [22], Saber [23], Alhaidery [24], Alhaidery [25], Zedan [26] . The proposed scheme achieves average TPR= 98.8, FPR= 3.5 in the GRIP

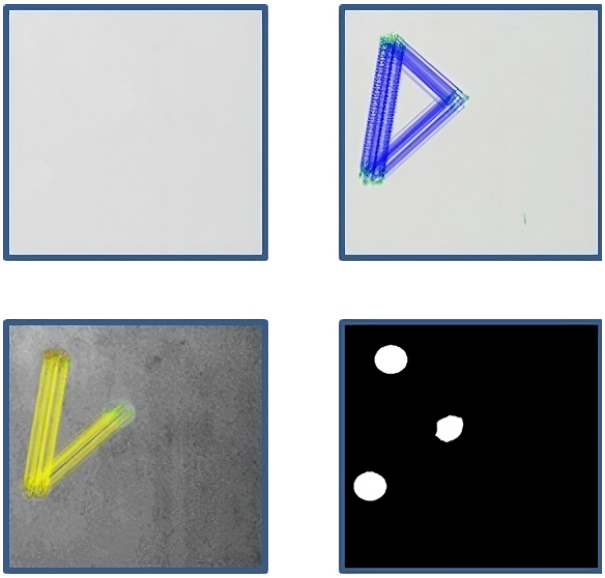


Fig. 6. Detection of multi duplicated regions undergone affine transformation and invisible regions. First row: (a) The source image, (b) After detection regions, Second row: (c) After filtering process, (d) localizing the duplicated regions.

dataset. To make a comparison in terms of TPR and FPR, as clarified in Table IV. and Fig. 7. On the other hand, we compared our scheme in terms of non-uniform transformation attacks, invisible duplicated regions and multi iterative regions to know the capability of the proposed scheme in Table V.

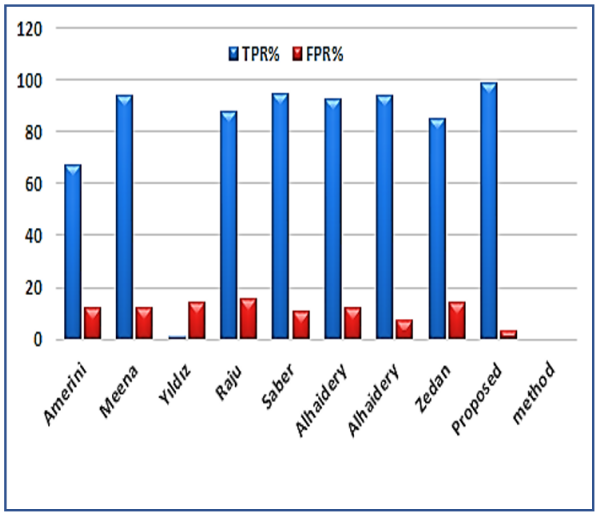


Fig. 7. TPR and FPR of proposed scheme and other schemes.

TABLE IV. COMPARISON TPR AND FPR RESULTS OF PROPOSED SCHEME WITH OTHER RECENT SCHEMES.

Methods	TPR	FPR
Amerini	67.13	11.89
Meena	94.12	12.3
Yıldız	89.8	14.2
Raju	87.5	15.5
Saber	94.57	10.5
Alhaidery1	92.5	11.8
Alhaidery2	93.75	7.25
Zedan	84.9	14
Proposed method	**98.8**	**3.5**

TABLE V. COMPARISON THE INVARIANT OF PROPOSED SCHEME WITH OTHER RECENT SCHEMES UNDER MAIN ATTACKS

CMFD schemes	Multi Clon.	Non-un.att.	Inv. att.
Amerini	Yes	No	No
Meena	Yes	No	No
Yıldız	Yes	No	No
Raju	Yes	No	No
Saber	No	No	No
Alhaidery1	Yes	No	No
Alhaidery2	Yes	No	No
Amiri [27]	No	No	No
Proposed method	**Yes**	**Yes**	**Yes**

VI. CONCLUSION AND FUTURE WORK

This article is about a passive image forensic scheme. A robust technique is presented to perform combined feature detection scheme. The scheme proposed to detect and locate single or multi duplicated regions in a digital image. We exploited Hessian-Affine and Harris-Affine as detectors and SIFT technique as descriptor to detect and describe enough features from target image. These detectors enhance the quality of the proposed scheme, which is invariant to photometric, uniform and nonuniform changes. In addition, our scheme able to detect the duplicated regions when them are small and invisible. We explained the performance of this scheme under simple and complex threatens then evaluate it based on TPR and FPR. The results and tables from image-level and pixel-level are demonstrated that both of TPR and FPR are encouraged and high. For future work, we will classify the detected regions into authentic and forged regions by merging machine learning approaches and deep learning approach like convolutional neural network (CNN).

CONFLICT OF INTEREST

The authors have no conflict of relevant interest to this article.

REFERENCES

[1] H. Kaur and N. Jindal, "Image and video forensics: A critical survey," *Wireless Personal Communications*, vol. 112, no. 2, pp. 1281–1302, 2020.

[2] I. A. Zedan, M. M. Soliman, K. M. Elsayed, and H. M. Onsi, "Copy move forgery detection techniques: a comprehensive survey of challenges and future directions," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021.

[3] M. M. A. Alhaidery, A. H. Taherinia, and H. S. Yazdi, "Cloning detection scheme based on linear and curvature scale space with new false positive removal filters," *Multimedia Tools and Applications*, vol. 81, no. 6, pp. 8745–8766, 2022.

[4] J. Fridrich, D. Soukal, J. Lukas, *et al.*, "Detection of copy-move forgery in digital images," in *Proceedings of digital forensic research workshop*, vol. 3, pp. 652–63, Cleveland, OH, 2003.

[5] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," 2004.

[6] J. Zhong, Y. Gan, J. Young, L. Huang, and P. Lin, "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools and Applications*, vol. 76, pp. 14887–14903, 2017.

[7] K. B. Meena and V. Tyagi, "A copy-move image forgery detection technique based on gaussian-hermite moments," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 33505–33526, 2019.

[8] 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 transactions on information forensics and security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[9] G. Gani and F. Qadir, "A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata," *Journal of Information Security and Applications*, vol. 54, p. 102510, 2020.

[10] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection.," *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[11] S. Satapathy and A. Joshi, "Information and communication technology for intelligent systems," *Proceedings of ICTIS*, vol. 1, 2018.

[12] C. Lin, W. Lu, X. Huang, K. Liu, W. Sun, H. Lin, and Z. Tan, "Copy-move forgery detection using combined features and transitive matching," *Multimedia Tools and Applications*, vol. 78, pp. 30081–30096, 2019.

[13] G. Gani, Z. Jeelani, and F. Qadir, "Cellular automata-based cmf detection under single and multiple post-processing attacks," *Multimedia Systems*, vol. 28, no. 1, pp. 257–266, 2022.

[14] F. Zare Mehrjardi, A. Latif, and M. Sardari Zarchi, "An optimal hybrid method to detect copy-move forgery," *Journal of AI and Data Mining*, vol. 11, no. 3, pp. 429–442, 2023.

[15] M. Hassaballah, A. A. Abdelmgeid, and H. A. Alshazly, "Image features detection, description and matching," *Image Feature Detectors and Descriptors: Foundations and Applications*, pp. 11–45, 2016.

[16] Y. Aydın, "A new copy-move forgery detection method using liop," *Journal of Visual Communication and Image Representation*, vol. 89, p. 103661, 2022.

[17] C.-C. Chen, W.-Y. Lu, and C.-H. Chou, "Rotational copy-move forgery detection using sift and region growing strategies," *Multimedia Tools and Applications*, vol. 78, pp. 18293–18308, 2019.

[18] T. Mahmood, A. Irtaza, Z. Mehmood, and M. T. Mahmood, "Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images," *Forensic science international*, vol. 279, pp. 8–21, 2017.

[19] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[20] G. Tahaoglu, G. Ulutas, B. Ustubioglu, and V. V. Nabiyev, "Improved copy move forgery detection method via l* a* b* color space and enhanced localization technique," *Multimedia Tools and Applications*, vol. 80, pp. 23419–23456, 2021.

[21] K. B. Meena and V. Tyagi, "A hybrid copy-move image forgery detection technique based on fourier-mellin and scale invariant feature transforms," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 8197–8212, 2020.

[22] P. M. Raju and M. S. Nair, "Copy-move forgery detection using binary discriminant features," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 2, pp. 165–178, 2022.

[23] A. H. Saber, M. A. Khan, and B. G. Mejbel, "Rdlnn-based image forgery detection and forged region detection using mot," *Karbala International Journal of Modern Science*, vol. 8, no. 4, pp. 596–606, 2022.

[24] M. M. A. Alhaidery and A. H. Taherinia, "A passive image forensic scheme based on an adaptive and hybrid techniques," *Multimedia Tools and Applications*, vol. 81, no. 9, pp. 12681–12699, 2022.

[25] M. M. A. Alhaidery, A. H. Taherinia, and H. I. Shahadi, "A robust detection and localization technique for copy-move forgery in digital images," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 449–461, 2023.

[26] I. A. Zedan, M. M. Soliman, K. M. Elsayed, and H. M. Onsi, "A new matching strategy for sift based copy-move forgery detection.," *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 4, 2023.

[27] E. Amiri, A. Mosallanejad, and A. Sheikhahmadi, "Copy-move forgery detection using an equilibrium optimization algorithm (cmfdeoa)," *Statistics, Optimization & Information Computing*, vol. 11, no. 3, pp. 677–684, 2023.