Tamper Detection in Digital Images Based on Key Points Features

AL- mustansiriyah University

Marwan Saad Kadhim / AL-Mustansiriyah University. Iraq

Email: Marwansaad٨٧٨٦@gmail.com

Dr.Eng. Heba Hatem

Email: heba.hatem@tishreen.edu.sy

Mechanical and Electrical Engineering – Telecommunications and Electronics department - Tishreen University .Syria

Abstract

The widespread adoption of digital image processing technology has been matched by advancements in image processing editing tools, facilitating the ease of changing and manipulating photographs. Nowadays, fake images that alter reality are becoming more common, whether it's done on purpose or by accident. Digital image fraud includes different types, and the Copy-Move technique is one of the most common and widely used types. This article introduces a novel approach for detecting instances of copy-move forgeries. The study employs the scale-invariant feature transforms (SIFT) approach for feature extraction. The proposed method was assessed by utilizing a set of ٢٠٠ images selected from the standard dataset known as MICC. The proposed method provided an accuracy of ٩٦,٥٪ which demonstrated improved accuracy and speed in detecting forgeries. Furthermore, the proposed method demonstrates resilience to various post-processing operations such as alterations in brightness, and blurring. Additionally, it effectively handles scenarios involving multiple copies.

Keywords: Copy-move forgery, Image tamper, Image tamper detection, Features extraction, Digital forensics.

١. Introduction

Images are commonly regarded as more effective than texts for human communication due to their immediate impact and ease of comprehension. The human visual system is capable of processing pictorial information more rapidly than other

forms of information [١]. Currently with the widespread of domains that rely on digital images like scientific journals, magazines, newspapers, courtrooms, fashion industry, and various additional domains [٢], Arise worries about some existing software that enables users to generate computer graphics that possess an indistinguishable resemblance to authentic images [٣].That is why, tracing and connecting the source of digital images to their creation procedure became fundamental procedure. The study of such questions has triggered the development of digital forensic photography. Digital forensics is a promising area to investigate which focuses on reforming incidents, detecting related objects, and evaluating the legitimacy and consistency of digital media. The idiom "forensic" means the set of methods and procedures put to investigate and find illegal digital activities [٥]. The procedures applied in digital image forensics fall under three categories: Computer Generated Image Detection, Image Source Identification, and Image Forgery Detection [٦]. The first approach deals with the ability of the system to detect manipulation and distinguish manipulated images from real ones. Figure ١ depicts a collection of computer-generated images. [٧].

Figure (١) Examples of computer-generated images [٧]

The second category in forensics takes into the account the source by which the image is generated, such as digital cameras or scanners. Although the operational mechanisms of imaging devices are understood, variations in the employed techniques lead to distinct traces or patterns in the resultant images. The significance of forensic techniques for digital images lies in their ability to verify patterns, uncover image authentication, and ascertain the source [٨]. The last one which is the focus of this research is Image Forgery Detection. Image Forgery is defined as the act of modifying the original image through various means such as copy-pasting, removal, addition,

resizing, rotation to any degree, enhancement, or combining multiple images to create a new [٩]. Now, images are easy to change and forged all that is due to the availability of creative image processing applications and editing tools like Adobe Photoshop, Affinity Photo and others. For that, there has been a lot of research to find methodologies that help in identifying digital alteration of images [١٠].

Figure (٢) the political enemy of Stalin was deleted [١١].

In Figure (٢) one can observe that the image has undergone a form of forgery known as copy-move forgery. This particular type of forgery involves the removal of Stalin's political adversary from the image using copying and pasting objects within the same image. The process of fabricating images in the past was a challenging and labor-intensive task due to the limitations of available tools and resources. In contrast, today, this process requires much less effort. A wide range of digital image processing and editing tools are now easily accessible, user-friendly, and powerful for users. The digital forensics discipline has been established with the primary aim of devising efficient and dependable techniques for detecting instances of image fraud [١٢] [١٣].

There exist five primary categories of image forgery, namely Copy-Move, Splicing, Retouching, Enhancing, and Morphing [٧]. The prevalent technique employed in image manipulation is known as copy-move forgery (CMF) or cloning, which is the focus of this research. (CMF) includes duplicating a specific portion or multiple portions of an image and then inserting these duplicated elements back into the original image. In figure (٣) one can forgery in which a truck was covered with a portion of the foliage left of the truck.

Figure (٣) Example of copy-move forgery, the original image at the left and the tampered image at the right [١٥].

Forgery involves the observation of various types of transforms, including rotation, scaling, translation, and combinations of all. In instances where rotation is employed, the component(s) undergo a process of copying, rotating, and moving (CRM) within the same image. Moreover, a variety of potential post-processing techniques, such as noise addition, color reduction, and image blur, can be proposed to enhance the realism of tampered images. The detection of tampering presents greater challenges compared to other forms. The ineffectiveness of conventional methods that employ statistical measurements to compare different segments of the image for detecting incompatibilities is the reason for this [١٦]. This research aims to develop and execute an algorithm for detecting copy-move forgery in digital image content using passive techniques. The algorithm should be capable of swiftly identifying instances of forgery, even after undergoing intricate transformations and post-processing operations. The proposed system will employ key-point methods, which are known for their distinctiveness and speed, while also minimizing unnecessary calculations. Instead of applying a fixed threshold to all images the dynamic threshold for each image will be computed using the low-frequency components.

The rest of the paper is organized as follows. Section ٢ will discuss related work in the area of study. Then, the methodology of the research will be presented in section ٣. Section ٤ will provide the results and the discussion of the research. Finally, the paper will end with the conclusion and future work.

٢. Literature review

Recently, the amount of research proposed on the detection and identifying digital image forgeries has notably increased. In a study targeting CMFD, The Discrete

Wavelet Transform (DWT) was used by Maj Outlaw Singh Mamba in ٢٠١٥. Fatima et al. (٢٠١٥) revised the algorithm proposed by Khan and Kulkarni. Kourtis et al. (٢٠١١) aimed to streamline management time within the organization. The Khan algorithm applies a discrete wavelet transform (DWT) to the input image, after which the compressed image is divided into overlapping blocks. These blocks are then organized row by row in cyclic arrays to check for any repetitions. Many of the subsequent improvements focus on eliminating redundant operations and exhaustive searches within the algorithm. Numerous experiments were conducted to identify appropriate threshold values for this method. The results indicate that the enhanced approach can effectively detect duplicated regions in the image. However, the literature review failed to address specific transformations, such as scaling and rotation.

In their study, Mishra and Rai (٢٠١٧) [١٧] introduced a technique for; Copy Move Forgery Detection (CMFD) that is based on "Two-dimension Principal Component Analysis" (٢D-PCA).A sliding window is initially centered within each block of an image. Next the window feature vector is obtained, and this is followed by storage of it in the feature matrix. The feature matrix is then sorted in lexicographic order so that similar windows will be located close together within this data structure. Copied regions are identified by utilizing adjacent pairs of feature vectors. However, this approach exhibits a relatively high time complexity.

In the study of Yang et al. (٢٠١٨) [١٨], they have introduced a CMFD strategy which combined the SIFT algorithm with a key-point distribution strategy that was aimed at getting even spreads of key points over images It can be found that it all codes are in the book Different and overlapping codes mean that lots of duplicate regions. However, this method also introduces an increased computational burden.

Chen et al. (٢٠٢٠) introduced a novelty detection approach for copy-move forgeries (CMF) using block-based methods. It is important to highlight that these techniques involve dividing an image into small, overlapping blocks. They then extract features from each block that remain invariant to processing across the entire image, creating resilient descriptors from its smallest representational elements. Based on this,

corresponding image blocks are matched and identified as potential areas of forgery. However, most block-based methods lack robustness against geometric transformation attacks and possess numerous features, leading to increased temporal complexities.

The study by Park and Choeh et al. (٢٠٢١) presents a novel method for detecting forged images that relies on geometric transformations, including area rotation, rescaling, distortion, and reflection. To identify copy-move forgeries, they extracted characteristic points from the image using the Scale-Invariant Feature Transform (SIFT) algorithm and generated corresponding descriptors for those points. The new algorithm is theoretically robust for Copy Move Forgery Detection and efficient in terms of processing time.

In their study, Mehrish et al. (٢٠٢٢) [٢١] block-matching technique was built on the Discrete Cosine Transform (DCT). To that end, the authors employ dot products to find the resemblance between the copied and pasted parts. In this approach, the target image is partitioned into overlapping blocks. And discrete cosine transform (DCT) coefficients are employed to extract relevant features.

The copy-move forgeries method duplicates and relocates a specific portion of an image within the same image to hide an important object. The emergence of new sophisticated forgery techniques also represents a steady challenge to image verification and integrity at large. Issues like time consumption, handling transformations, shifting pixels, and many others are challenging. In this study, a passively detecting copy-move forgeries method in digital image content is built and applied. Even with complicated transformations and processing alterations, the algorithm is able to rapidly identify occurrences of forgery. It deals with scenarios in which there are many copies of the fake image.

٣. Methodology

The schematic representation of the suggested approach is illustrated in Figure ٤. Initially, the input image is converted to grayscale. The SIFT technique is used to extract key-point features and their corresponding descriptors. Subsequently, the k-nearest neighbors of each key point are identified, and the matching key points that

meet the specified requirements are determined. Our approach managed to decrease the false positives results.

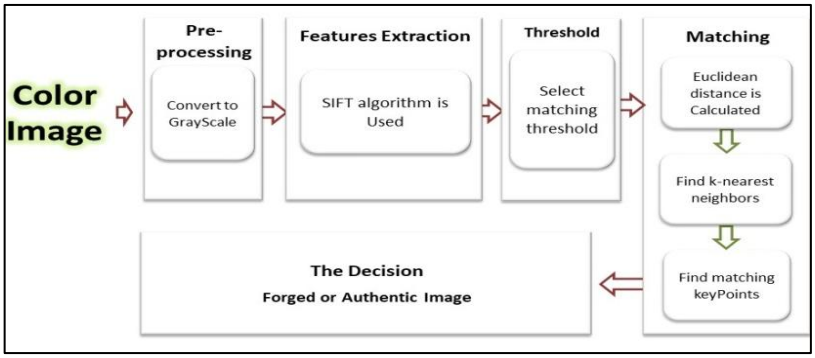


Figure (٤) Block Diagram of the Proposed CMFD Algorithm Phases

The figure above outlines the four phases of our proposed method, beginning with Pre-processing, followed by Feature Extraction and Matching Processes, and concluding with the Decision phase.

The following sections part provides a comprehensive overview and explanation of each step.

٣,١ . Preprocessing

This step encompasses two distinct procedures: Grayscale Conversion and Automatic Threshold Computation.

٣,١,١ Grayscale Conversion

The first step is the conversion of the color picture into grayscale.

٣,١,٢ Threshold Selection

The threshold for matching between feature vectors is a crucial parameter in the context of CMFD. The selection of the matching threshold (T) and minimum distance was carried out using experimental methods, resulting in a threshold value of T at ٠,٤٥ and a minimum distance of ٣٥.

٣,٢ Features Extraction

Several key aspects can be identified to offer a thorough representation of the visual attributes. The Scale-Invariant Feature Transform (SIFT) technique can generate a significant number of features when utilized. These features remain invariant under

various conditions and possess a distinct quality. The likelihood of finding a match between a single feature and a feature database is quite high. Algorithm ٣ details the steps involved in the feature extraction phase using the SIFT technique

Algorithm ٣: Features Extraction.
Input: Grayscale image.
Output: Key-points descriptors, Key-points locations.
Begin - Step ١: Convert grayscale image. - Step ٢: A scale space is constructed by creating many scales of the original image. - Step ٣: For each octave: Create Gaussian blur intervals. Create difference-of-Gaussian intervals. - Step ٤: Find key-points that are local extrema. - Step ٥: weak key points are eliminated by removing the low-contrast regions. - Step ٦: Assign an orientation to the key points. - Step ٧: Key-points descriptors and locations are generated. End

In this stage, the SIFT technique is employed to extract the important key points from the image. Each key point consists of two elements: a location vector and a descriptor vector. Each key point is represented by a ١٢٨-dimensional descriptor vector, and the number of key points extracted can vary. The positions of the key points and their associated descriptor vectors are stored in a matrix. Subsequently, the computation of the extracted key points is carried out.

٣,٣ Matching Processes

The matching procedure used in the algorithm utilizes SIFT characteristics. In instances of copy-move forgeries, the key points derived from both the copied regions and the original regions exhibit comparable descriptor vectors. Hence, it is very suitable for detecting instances of copy-move forgeries. The algorithm ٤ provides a representation of the primary phases involved in the matching phase [٢٣].

Algorithm ٤: Matching of key points.
Input: Key-point descriptors, Key-point location Matching threshold, Mini distance threshold.
Output: Candidate matches.
Begin - Step ١: Compute the Euclidean distance for each key point with others. - Step ٢: Find the first ١٥ nearest neighbors for each key point. - Step ٣: Find matching key points as follows: For each key point; For G = ١ to ١٥ Begin Find d١ is the Euclidean distance between a key-point and the G-neighbors. Find d٣ is the Euclidean distance between a key-point and the G+٢ neighbors. Save the coordinates of the matched key points which satisfy the: $\frac{d1}{d3}$ < Matching threshold. key-point location and G-nearest neighbors > distance threshold. End End

Potentially more efficient methodology may be achieved by using the ratio between the distances of the first closest neighbor and the second nearest neighbor, afterward evaluating this ratio against a predetermined threshold, often referred to as the G٢NN test. The two key points are deemed to be matched only when the following restriction, as shown in Equation ١, is met.

$$\frac{d1}{d2} < T \qquad \dots (١)$$

Where:-

d١ is the Euclidean distance between a descriptor of key-point and G-nearest neighbors.

$d^{٢}$ is Euclidean distance between a descriptor of key-point and G+١ nearest neighbors. T is the determined matching threshold.

The concept of testing $G^{٢}$NN may be described as follows: when a match is found, the ratio between the distance of the matched candidate and the distance of the second closest neighbor is quite small. In the event of two randomly selected characteristics, the resulting ratio will have a significant magnitude. To address this particular scenario, the matching process used is a generalized version known as the $G^{٣}$NN test, which is capable of effectively handling multiple copies. The two key points are deemed to be matched only when the condition outlined in Equation ٢ is met.

$$\frac{d1}{d3} < T \qquad \dots (٢)$$

Where:

$d^{١}$ is Euclidean distance between a descriptor of key-point and G-nearest neighbors (GNN),

G is ١, ٢…١٥.

The $d^{٣}$ is Euclidean distance between a descriptor of key-point and G+٢ nearest neighbors (G+٢NN).

T is the selected match threshold.

To enhance the precision of the matching process, a micro distance condition has been included. The distance between the locations of the two matching key points must exceed the minimum distance requirement; otherwise, it should be disregarded.

$$d \text{ (key-point Location and GNN)} > \text{mini distance} \qquad \dots (٣)$$

Where:

d is the Euclidean distance between key-point Location and GNN.

GNN is G-nearest neighbor.

G is ١, ٢…١٥.

Ultimately, via the process of iterating this particular method on each key point, the resultant collection of matching key points may be acquired. This enables the

identification of duplicated locations, hence facilitating the detection of picture tampering.

٣,٤ The Decision making step (Forged or Authentic Image)

The concluding stage of the algorithm under consideration presents the outcome of the input image. If there are no corresponding key points, the input image will be shown as an unaltered image. On the contrary, if there are corresponding key points, the input image will be classified as a manipulated image.

٣,٥ Evaluation Metrics

In order to evaluate the performance of the proposed system a set of evaluation metrics were used. These metrics include Recall, Precision, F١-Score, True Negative ratio, false positive ratio, false negative ratio and accuracy. Their equations are listed as follows:

$$\text{Recall} = \frac{TP}{TP+FN} \quad (٤)$$

$$\text{Precision} = \frac{TP}{TP+FP} \quad (٥)$$

$$\text{F١ Score} = \frac{٢\ X\ precision\ X\ recall}{precision+\ recall} \quad (٦)$$

$$\text{TNR (True Negative Rate) (Specificity)} = \frac{TN}{TN+FP} \quad (٧)$$

$$\text{FPR (False Positive Rate) (١- specificity)} = \frac{FP}{FP+TN} \quad (٨)$$

$$\text{FNR (False Negative Rate) (١- sensitivity)} = \frac{FN}{FN+TP} \quad (٩)$$

$$\text{Accuracy} = \frac{TP+\ TN}{TP+FN+TN+FP} \quad (١٠)$$

٤. Results and Discussion

This section presents the implementation findings of the proposed Copy-Move forgery detection system, as well as an investigation into the impact of various thresholds on the system's performance.

The system of our proposal was successfully implemented using Windows ١٠ operating system and MATLAB R٢٠٢٠a. The use of the VLFeat library, which is C++ based and focuses on image interpretation and local feature extraction, increases the efficiency executing the SIFT algorithm.

The model is then used to analyze ٢٠٠ carefully selected images from an existing dataset, specifically the MICC dataset [١٩]. The results are expressed by calculating True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) in tables. This chapter will explain and show the experiment, results, and comparison with other methods.

٤,١ Dataset of Image Forgery

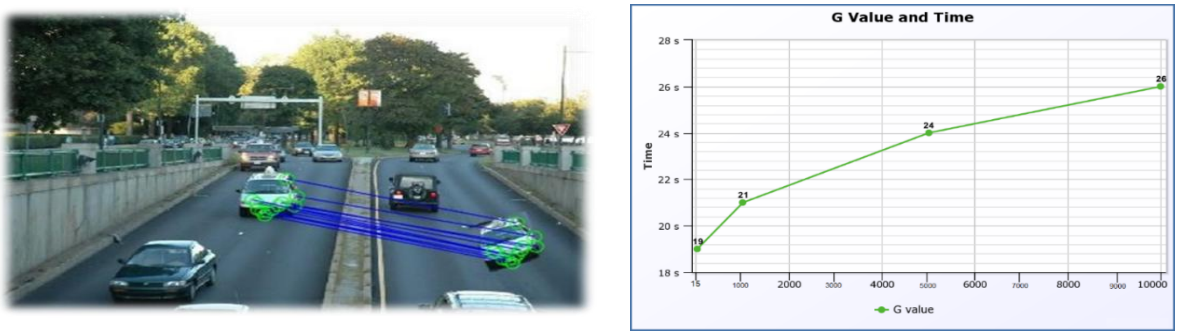
Data from the Florence University, Media Integration and Communication Centre, the MICC-F٢٢٠ dataset were used to evaluate the methodology referred to above. MICC-F٢٢٠ dataset consists of ٢٠٠ images in total, half of which are tampered and the other half original photos. Figure ٥ presents representation a of several instances of manipulated photographs from the MICC dataset. The generation of counterfeit images involves the process of duplicating arbitrary sections of an image and subsequently integrating them back into the original image. Various forms of manipulation have been employed to alter fabricated images, including rotation, translation, scaling, or a combination thereof. The datasets consist of images with varying dimensions, presented in the JPEG image format.

Figure (٥) some examples of the tampered images of MICC.

٤,٢ The experiment of G-Nearest Neighbors (GNN)

The technique of comparing any key points involves comparing them to their nearest neighbors, also known as (GNN). Determining the value of G depends on the specific application at hand. An increase in the value of G leads to a corresponding increase in the number of comparisons, which leads to an increase in execution time. Likewise, a decrease in the value of G would lead to a decrease in the number of

comparisons and a subsequent decrease in execution time. The greater the value of the parameter G, the greater the number of points that will be compared, and thus there will be an increase in the number of comparisons. To achieve a balance between the amount of time necessary for processing and the number of comparisons needed. Multiple values of G have been tested to determine the optimal one. Figure ٦ a. depicts the tamper present in the image, while Figure ٦ b. demonstrates the impact of increasing the G value on the processing time of the image.



a) **b)**

Figure ٦ a. Tamper detection in the forged image. b. The effect of increasing G value time.

Figure ٦ b. demonstrates a positive correlation between the G value and the processing time, indicating that an increase in the G value leads to an increase in processing time. After conducting multiple experiments, the value of the gravitational constant, denoted as G, has been proven to be ١٥. By following this principle, the required comparisons will be conducted within an optimal processing time. It is unlikely to find the corresponding key points beyond the ١٥th neighboring data point. As a result, any further comparisons will be considered ineffective and unlikely to yield beneficial results.

٤,٣ Visual Results

The algorithm under consideration has undergone testing using a sample of ٢٠٠ images selected from the MICC- MICC-F٢٢٠ datasets [١٩]. Figures ٧ depict a selection of original and manipulated photographs utilized during the testing process.

Figure ٧ the detection results for tampering images under different transformations.

The tested image collection is comprised of two distinct components: The initial segment comprises a collection of ١٠٠ authentic images that have not undergone any form of alteration or tampering. The subsequent segment comprises a collection of ١٠٠ fabricated images, each exhibiting distinct forms of tampering through various transformations, including translation, rotation, scaling, and combinations of all. Table (١) illustrates the results of proposed system.

Testing of the proposed system			
TP	TN	FP	FN
٩٦	٩٧	٣	٤

Table ١ the final results of the testing process

٤,٤ Discussion

This section will provide an overview of the various proposed methods and compare them with relevant literature. Fatima et al. [٧] suggested improvements to the Khan and Kulkarni algorithm [٢٤]. Although our current approach does not address issues such as copy-rotation or copy-scaling and it focuses solely on instances of copy-pasting. However, the method outlined in this paper can effectively manage these types of forgeries due to the extensive modifications made. It is applicable to copy-move, copy-rotate, and copy-scale scenarios, potentially offering greater effectiveness than other previously examined methods. The manipulated images used were generated using copy-rotate and copy-scale techniques, as illustrated in Figure ٨.

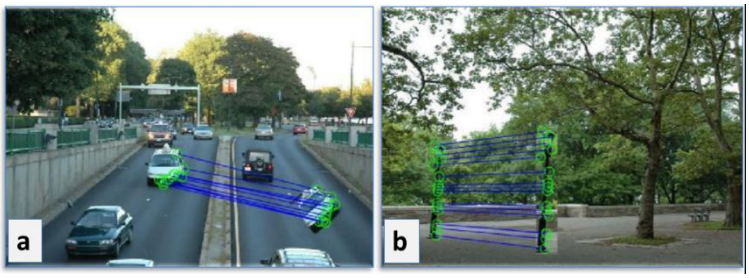


Figure ٨ Identifying of tamper in the forged photos.

A. Copy-rotate forgery. b. Detection of the copy-scale forgery.

The proposed technique was evaluated on the same set of photos utilized in the study conducted by Fatima et al [٧], to determine the duration required for forgery detection. The comparison procedure depicted in Figure ٩ demonstrates the utilization of a horizontal axis to represent the picture number and a vertical axis to represent the time in seconds.

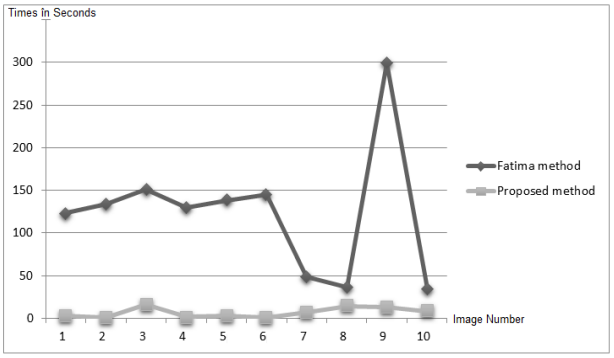


Figure ٩ the comparison of the processing time of the proposed method and Fatima's method.

The presented figure demonstrates that the proposed algorithm exhibits enhanced speed and reduced processing time throughout the detection process as compared to the Fatima technique. The method of comparing the proposed algorithm with other related works is depicted in Table ٢.

The Authors	The Accuracy
Fadl and Semary [٢٥]	٧٨,٢٥ %
Jen-Chun Lee [٢٦]	٨١ %
J.C. Lee et al [٢٧]	٩٠ %
V. Parihar et al [٢٨]	٩٠ %
T. Das et al [٢٩]	٩٣ %
B. Yang et al [٣٠]	٩٥,٨٨ %
The proposed	٩٦,٥ %

Table ٢ the comparison process between the proposed algorithm and other related work

٥. Conclusion

The rapid advancement of image processing techniques has sparked increased interest in the field of image forensics, particularly in detecting digital image forgery. The issue of image forgery, specifically the copy-move technique, has become a significant challenge in digital image forensics. There is a substantial amount of research dedicated to detecting copy-move forgery, with ongoing efforts to advance this area of study. However, many existing methods demonstrate considerable temporal complexity. The technique developed in this study focuses on detecting instances of copy-move forgery using key-point approaches. This algorithm offers the benefit of reduced computational complexity, enabling quick detection of forgeries. Moreover, its effectiveness in identifying forgeries remains strong, even when faced with various modifications or multiple instances of duplication. For future work, we suggest enhancing the system's performance by exploring alternative approaches to establish threshold values or incorporating segmentation techniques during the matching process. Additionally, it is advisable to consider a different algorithm for feature extraction. And using machine learning models is also recommended.

References

[١] M. Sivakumar, P. Roy, K. Harmsen, and S. Saha, "Satellite remote sensing and GIS applications in agricultural meteorology", in Proceedings of the Training Workshop in Dehradun, India. AGM-٨, WMO/TD, no. ١١٨٢, ٢٠٠٤.

[٢] B. Shivakumar and S. Baboo, "Detection of region duplication forgery in digital images using SURF", IJCSI International Journal of Computer Science Issues, vol. ٨, no. ٤, p. ١٩٩, ٢٠١١.

[٣] A. Swaminathan, M. Wu, K. Liu, "Digital image forensics via intrinsic fingerprints", IJCSI International Journal of Computer Science Issues, vol. ٣, no. ١, pp. ١٠١-١١٧, ٢٠٠٨.

[٤] Z.-N. Li, M. S. Drew, and J. Liu, "Fundamentals of multimedia, Second Edition", Springer, ٢٠٠٤.

[٥] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", Forensic Science International vol. ٢٣٣, no. ١-٣, pp. ١٥٨-١٦٦, ٢٠١٣.

[٦] J. Redi, W. Taktak, and J.Dugelay, "Digital image forensics: a booklet for beginners", Multimedia Tools Appl vol. ٥١, no. ١, pp. ١٣٣-١٦٢, ٢٠١١.

[٧] F. O. Haimour, M. A. Khraiwesh, and K. W. Mahmoud", An Improved Method for Detecting Copy-Move Forgery in Digital Images," Master Thesis, Zarqa University, ٢٠١٥.

[٨] Y. Huang, L. Cao, J. Zhang, L. Pan, and Y. Liu, "Exploring feature coupling and model coupling for image source identification", IEEE Transactions on Information Forensics and Security vol. ١٣, no. ١٢, pp. ٣١٠٨-٣١٢١, ٢٠١٨.

[٩] M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review", IETE Journal of Education vol. ٥٥, no. ١, pp. ٤٠-٤٦, ٢٠١٤.

[١٠] B. Sarma and G. Nandi, "A Study on Digital Image Forgery Detection", International Journal of Advanced Research in Computer Science and Software Engineering vol. ٤, no. ١١, ٢٠١٤.

[١١] N. Diane, W. Nanda, S. Xingming, and F. Moise, "A survey of partition-based techniques for copy-move forgery detection", Hindawi Publishing Corporation vol. ٢٠١٤, ٢٠١٤.

[١٢] V. Parihar and B. M. Mehtre, "Copy Move Forgery Detection Using Key-Points Structure", Master Thesis, SARDAR PATEL UNIVERSITY OF POLICE, SECURITY AND CRIMINAL, ٢٠١٦.

[١٣] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques", International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. ١-٧: IEEE ٢٠١٧.

[١٤] B Shivakumar and S. Baboo, "Automated forensic method for copy-move forgery detection based on Harris interest points and SIFT descriptors", International Journal of Computer Applications, vol. ٢٧, no. ٣, pp. ٩-١٧, ٢٠١١.

[١٥] a Jessica Fridrich, b David Soukal, and a Jan Lukáš , Detection of Copy-Move Forgery in Digital Images, Department of Electrical and Computer Engineering, Binghamton, NY ١٣٩٠٢-٦٠٠٠

[١٦] S. Walia and K. Kumar, "Digital image forgery detection: a systematic scrutiny", Australian Journal of Forensic Sciences, pp. ١-٣٩, ٢٠١٨.

[١٧] M. Mishra and P. Rai, "A Proposed Work on Image Forgery Detection Technique", International Journal of Computer Applications vol. ١٦٣, no. ٢, ٢٠١٧.

[١٨] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT", Multimedia Tools and Applications: Springer, vol. ٧٧, no. ١, pp. ٨٣٧-٨٥٥, ٢٠١٨.

[١٩] Chen, Haipeng, Xiwen Yang, and Yingda Lyu. "Copy-move forgery detection based on keypoint clustering and similar neighborhood search algorithm." IEEE Access ٨ (٢٠٢٠): ٣٦٨٦٣-٣٦٨٧٥.

[٢٠] Khudhair, Zaid Nidhal, Farhan Mohamed, and Karrar A. Kadhim. "A review on copy-move image forgery detection techniques." Journal of Physics: Conference. Vol. ١٨٩٢. No. ١. IOP Publishing, ٢٠٢١.

[٢١] Singh, Richa, et al. "Copy-move Forgery Detection using SIFT and DWT Detection Techniques." ٢٠٢٢ ٣rd International Conference on Intelligent Engineering and Management (ICIEM). IEEE, ٢٠٢٢.

[٢٢] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review", Australian Journal of Forensic Sciences, vol. ٤٩, no. ٣, pp. ٢٨١-٣٠٧, ٢٠١٧.

[٢٣] M. A. Qureshi and M. J. Deriche, "A bibliography of pixel-based blind image forgery detection techniques", Signal Processing: Image Communication, vol. ٣٩, pp. ٤٦-٧٤, ٢٠١٥.

[٢٤] S. Khan and A. Kulkarni, "Robust method for detection of copy-move forgery in digital images", International Conference on Signal and Image Processing, pp. ٦٩-٧٣: IEEE, ٢٠١٠.

[٢٥] S. M. Fadl and N. A. Semary, "A proposed accelerated image copy-move forgery detection", IEEE Visual Communications and Image Processing Conference, pp. ٢٥٣-٢٥٧: IEEE, ٢٠١٤.

[٢٦] J.C. Lee, C.P. Chang, and W.K Chen, "Detection of copy–move image forgery using histogram of orientated gradients", Information Sciences, vol. ٣٢١, pp. ٢٥٠-٢٦٢, ٢٠١٥.

[٢٧] J. C. Lee "Copy-move image forgery detection based on Gabor magnitude", Vis. Commun. Image, vol. ٣١, pp. ٣٢٠-٣٣٤, ٢٠١٥.

[٢٨] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD-New database for copy-move forgery detection", in Proceedings International Symposium ELMAR, pp. ٤٩-٥٤: IEEE, ٢٠١٣.

[٢٩] T. Das, M. Azam, and R. Hasan, "SWT and SIFT based copy-move image forgery detection", BRAC University, ٢٠١٧.

[٣٠] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT", Multimedia Tools and Applications: Springer, vol. ٧٧, no. ١, pp. ٨٣٧-٨٥٥, ٢٠١٨.