Copy-Move Forgery Detection and Localization Using Novel Technique

Ms. Preeti Kale [#1], Dr. Vijayshree A. More[*2], Dr. Ulhas B. Shinde[#3]
[1]PhD Student, Dr. Babasaheb Ambedkar Marathawada University, Aurangabad.Maharashtra,India
[2]Associate Professor, MGM'S Jawaharlal Nehru Engineering College, Aurangabad.Maharashtra,India
[3]Principal,Chh.Shahu College Of Engineering,Aurangabad, Maharshtra,India.
p.gajanan@rediffmail.com vijayshreemore@gmail.com,drshindeulhas@gmail.coml

Article Info
Page Number: 1173 – 1186
Publication Issue:
Vol. 71 No. 3 (2022)

Abstract
Nowadays, Image Forgery is the most extensively exploited security vulnerability in real-time applications. It necessitates the approach to discover such vulnerabilities using computer vision mechanisms. The Copy-Move Forgery has commonly appeared the image forgery in multimedia applications. Several Copy-Move Forgery methods have already been proposed for forgery detection and localization. The majority of the approaches fell short of achieving maximal precision with correct forgery localization. Other techniques have suffered from a significant computation burden. To end this, we proposed novel image forgery detection and localization framework. The proposed framework is called GFGIF (Guided Filtering with Geometric Invariant Features) for robust and accurate forgery detection and its localization. The GFGIF consists of two phases such as forgery detection and forgery localization. For forgery detection, we pre-processed the input image using a guided filter and then decomposed it into non-overlapping blocks. The Geometric Invariant features are extracted from each block. Using Euclidean Distance measure, we first discovered the candidate blocks and then detected the forgery blocks. Localization of forged blocks efficiently is another challenge for further analysis purposes. We accurately localize the forged objects in the image using the detected forged blocks. The simulation results show the efficiency and robustness of the proposed model compared to state-of-art methods.

Keywords: -Copy-move forgery, forgery detection, forgery localization, guided filtering, geometric invariant features, candidate blocks.

Article History
Article Received: *12 January 2022*
Revised: *25 February 2022*
Accepted: *20 April 2022*
Publication: *09 June 2022*

1. Introduction

Image forgery is a widespread problem that has a severe influence on society. Previously, it did not impact the general population since sophisticated software and editing tools were not readily available; however, the rapid advancement of image processing software has made this operation very straightforward [41]. When a picture is doctored with care, it is difficult for people to tell whether it is original or doctored. In today's digital world, image authenticity is extremely important. Cloning doctoring is a simple form of tampering in which an item is copied and pasted into another location within the same picture in order to obscure some of the image's vital elements. It is difficult for the human visual framework to tell if a digital image is authentic or doctored if image forging is done carefully without leaving any evidence. Furthermore, the rapid advancement of digital image processing

software and the internet has made this operation very simple; anybody may readily doctor digital images utilising these easily accessible editing softwares. These patterns show a high level of vulnerability, as well as a reduction in the trustworthiness of digital photographs [5]. As a result, new algorithms for certifying the integrity and persuasiveness of digital pictures should be created. It is also quite significant in today's digital environment, particularly obtaining in this respect the image is granted as evidence in a court of law, as financial papers, as a part of medical records, and may be used in a variety of other important locations. As a result, detecting digital forgeries is crucial [10].

Cloning forgery is the most popular sort of image forgery, and it is widely used to corrupt digital images. Furthermore, in cloning, an item or a piece of an image is duplicated and pasted onto another area of the same image to hide an important characteristic. Because the cloned area has the same features as the original picture, such as texture, noise component, and colour palette, the process of identifying image counterfeiting becomes more difficult. Furthermore, these qualities suggest that using discrepancies in statistical measurements as a detection strategy for copy-move forgeries would fail [44] [2]. There are a variety of strategies that may be used to solve the problem of copy-move image forgery. These methods provide a result based on a set of conditions and assumptions; however, if these assumptions are not met, these methods will fail. The direct approach for clone identification divides the picture into small overlapping blocks, which are then compared to one another. If two blocks are proven to be identical, these blocks are likely forgeries. There are ((s-m+1) (s-p)/2) p2 comparisons if the picture has ss pixels, the block size is pp pixels, and the blocks are compared pixel by pixel.There are 7.4 million comparisons if s=256 and p=16. As a result, we may conclude that these direct approaches are too slow to detect doctoring in digital photographs.

Various academics have given a variety of automated algorithms for detecting copy-move forgeries. Essentially, copy-move forgery resulted in a correlation between the original and faked picture regions [43]. For reliable identification of such sorts of counterfeit, such a correlation factor is used. Due to the lossy JPEG format and the usage of various scaling and retouch picture processing techniques, the identified counterfeit regions may not be precisely located. (1) Algorithm for forgery detection must do approximate matching of small regions of image, (2) Algorithm must work quickly with more accuracy and less errors, and (3) Forged region of image must be represented in form of connected component rather than small pixels, according to the requirements for copy-move forgery detection [42]. Despite the fact that several new strategies for copy-move forgery detection have been proposed in digital image processing, there are still key traps to avoid when creating an efficient forgery detection method. We aim to create unique algorithms for copy move forgery detection under various picture lighting situations in this research.

Since the arrival of Internet of Things (IoT) across the different applications, there is possibility of multimedia data threats. It is necessary to devise a method for verifying the authenticity or originality of an input digital image that is both efficient and reliable. Many similar strategies have recently been presented by researchers for the detection of copy-move forgeries. The major goal of such systems is to accurately detect or locate fabricated regions. The majority of the strategies were unsuccessful in achieving performance trade-offs. Some approaches are more accurate, but they take longer to detect [34]. Many approaches were

developed that used feature extraction techniques like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Scale Invariant Feature Transform (SIFT), and block-based techniques like overlapping blocks and non-overlapping blocks, as well as block-based techniques like overlapping blocks and non-overlapping blocks. The majority of approaches used in current research are based on blocking, wavelet transformations, and classifiers, among other things. However, with recent advancements in digital technology, several research issues have arisen in detecting copy-move forgeries rapidly and reliably. Recent SIFT, Singular Value Decomposition (SVD), DWT, and other forgery detection technologies have failed to yield good results [32]. For example, the amount of matching key points or blocks may be insufficient to establish that a picture is a copy-move forgery image. For high-quality photos, most blocking-based forgery detection and localization methods have large processing costs. Some existing forgery detection approaches were ineffective in detecting counterfeit segment localization findings [33]. To end this, we have proposed the novel GFGIF framework with the goal of robust and efficient forgery detection and localization using guided filtering with geometric invariant features. We have integrated the mechanism of digital image pre-processing with a block-based approach, block-based features extraction, block-based thresholding, block-based forgery detection, and localization. Section 2 presents the review of some recent works. Section 3 presents the proposed methodology. Section 4 presents the simulation results and discussions. Section 5 presents the conclusion and future works.

2. Related Works

This section presents the study of some recent copy-move forgery detection methods. The author presented blind detection and localization of copy-move fraud in [25]. One of the most important procedures is the Voice Activity Detection (VAD) module, which analyses audio recordings to detect and find frauds. The VAD module was also critical in the development of the copy-move forgery database, which included audio samples generated from several types of microphone recordings. Unlike other wavelet transforms (e.g., discrete wavelet transform), stationary wavelet transform (SWT) is shift-invariant and aids in the discovery of similarities, i.e., matches, and dissimilarities, i.e., noise, between picture blocks generated by blurring [16]. The blocks were represented by features extracted from a photograph using SVD.Based on the block matching approach, the author published a 2D-DWT-based copy-move forgery detection system in [17]. They employed DWT to deconstruct the image, which was then followed by different chunks. To detect fraudulent blocks, they employed the SVD for feature extraction. Using a block-based technique, the author created yet another novel way for identifying copy-move forgeries in [18]. They divided the image into several overlapping blocks using pre-processing first, then circular blocks computation. To extract the traits, they employed DRHFMs (Discrete Radial Harmonic Fourier Moments).The author presented a keypoint-based and block-based hybrid technique to detecting copy-move fraud in [19]. The block-based approach was used to locate forged key points, and the pixel-based method was used to localize the forged regions. They developed BDF for feature extraction (Binary Discriminative Feature Descriptor). The author of [20] proposed detecting copy-move fraud by dividing the image into smooth and textural parts. They extracted and matched texturing areas' essential spots. They used non-overlapping blocks as candidate blocks in smooth areas.

In [1], the author proposed using DCT to detect copy-move changes in a photograph. The transfer vector may be produced using the characteristics determined from DCT coefficients. To detect the fraudulent regions, they used a threshold.

In [14], the author presented a rapid and efficient copy-move forgery detection strategy that includes adaptive key point extraction and processing, providing a fast robust invariant feature, and removing the inaccurate pairs. Based on crucial considerations, the authors of [15] suggested an improved region duplication detection technique. The suggested technique makes use of the SIFT (scale-invariant feature transform) and reduced LBP (local binary pattern) histograms. LBP values of 256 levels were obtained from the local window centered on the key point before being reduced to 10 levels. The authors of [1] recommended for the use of DCT to detect copy-move forgeries. The properties generated from these coefficients allowed for the creation of transfer vectors, which were then aggregated. Using a tolerance threshold, it was possible to determine if there were chunks copied and pasted inside the inspected image. The authors of [9] suggested yet another recent copy-move forgery detection algorithm that is independent of the falsified areas' features. SIFT key points were extracted from CLAHE applied sub-images utilizing RGB and L*a*b* colour spaces from the input image. The authors of [4] proposed two deep learning approaches: a custom architectural model and a transfer learning model. The impact of network depth was measured in terms of precision, recall, and F1 score in each scenario. To identify and locate photo counterfeiting, the authors of [3] advised using deep learning and semantic segmentation. Color illumination was used to apply the colour map after the pre-processing step. The authors of developed another recent solution for picture authentication in [28]. They used the DCT for copy-move forgery detection. The properties derived from these coefficients allowed for the creation of transfer vectors, which were then combined together. They used a tolerance level to detect if forgery areas were present in the analyzed picture. To address the aforementioned issues, the authors of [29] suggested a powerful copy-move forgery detection approach. For copy-move forgery detection, the suggested approach used a combination of accelerated robust features (SURF) and binary robust invariant scalable key points (BRISK) descriptors. The authors of [30] presented a DCT and SVD-based technique for detecting copy-move fraud. They employed DCT to convert the picture from the spatial to the frequency domain. SVD was used for the feature dimension reduction.

The fundamental research topic among all of the approaches discussed above is the performance trade-off between recognising the accurate forging locations and computing efficiency. When precision, efficiency, and durability are all required, accurate forgery detection remains a nightmare. To conclude, we suggested a new Guided Filtering and Geometric Invariant Features technique for minimising processing needs while maximizing forgery detection accuracy across many datasets [31] [32]. Furthermore, we have extended the mechanism of forgery detection for the accurate forgery regions localization on the input digital image.

3. GF-GIF Methodology

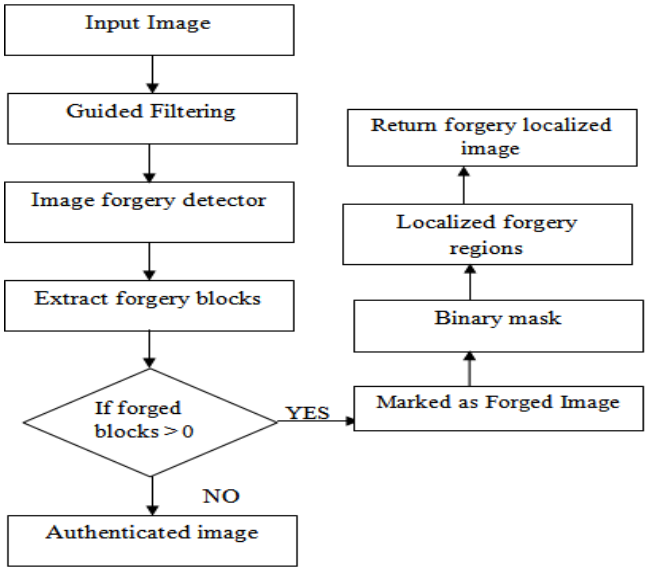

Figure 1. Proposed Architecture For The Copy-Move Forgery Detection And Localization

This section presents the mechanism of the proposed model GF-GIF for efficient and robust copy-move forgery detection and localization. Figure 1 shows the overall architecture of the proposed model. Broadly GF-GIF model consists of two phases as image forgery detector and image forgery localization. The input digital image has first pre-processed using the GF mechanism. The pre-processed GF image has then decomposed into several non-overlapping blocks.

The blocks are further processed by extracting the geometric invariant features from each block. The extracted blocks are sorted lexically to discover the candidate blocks. The candidate blocks are extracted using the pre-defined threshold. Once the candidate blocks are extracted, we used them for detecting the forgery blocks in the original image. This can be done by computing the Euclidean distance measure between the candidate block to each block and then applying another predefined threshold value to determine the forgery blocks. If the image has any forgery block, then it is marked as the forgery image, otherwise marked as the original and authenticated image. If an image is detected as the forgery image, then we have launched the forgery region localization.

We have used the binary mask to localize the extract RGB forgery blocks in the original input image. We have set the threshold value 0.7 according to experimental investigations using the different datasets. Algorithm 1 shows the complete functionality of the proposed model.

Algorithm 1: Copy-Move Forgery Detection and Localization
I: $input\ color\ image$ b: $blocksize$ $T1 = 0.7$ $T2 = 0.7$ I^{forg}: $Output\ forgery\ detected\ image$
Select the input image I $I^1 = rgb2gray(I)$

$I^2 = guidedFiltering(I^1)$
$B^{nonoverlap} = getBlocks(I^2, 'distinct', b)$
For each block$j \in B^{nonoverlap}$
$fr = getGIF(j)$
$B^{GIF} = [B^{GIF}, fr]$
End For
Perform the lexical sorting
$B^{sort} = lexicalSort(B^{GIF})$
Extract the candidate blocks
For each block $i = 1\ to\ (size\ (B^{sort}) - 1)$
$D1 = dist(B^{sort}(i), B^{sort}(i+1))$
If $(D1 > T1)$
$CB\ (:)\ = B^{sort}(i),$
End If
End For
Detect forgery blocks using candidate blocks
$forgery_{count} = 0$
For each block $i = 1\ to\ size\ (B^{GIF})$
For each block $j = 1\ to\ size\ (CB)$
$D2 = getDist\ (B^{GIF}(i), CB(j))$
If $(D2 > T2)$
$forgery_{count} + +$
$B^{nonoverlap}(i) = 0, (Mark\ this\ block\ as\ forgery)$
End If
End For
End For
If $(forgery_{count} > 0)$
$I^{forg} = transform(B^{nonoverlap})$
Generate the binary mask $I^{mask} = binarymask(I^{forg})$
Localize the regions in RGB image
$I^{localize} = I - I^{mask}$
End If
$Return\ (I^{localize})$
$Stop$

The input image I^1 first pre-processed using the guided filtering function called $guidedFiltering(.)$. This function returns the pre-processed image I^2. The canny edge detection used to generate the guidance image for input source image as:

$$G = edgeDetector\ (I^1, 'canny') \quad (1)$$

Where, G is guidance image generated by edge detector function of input I^1image. After generating guidance image G, next step is to apply the guided filter by:

$$I^2 = GFF\ (I^1, G, \epsilon,\ winsize) \quad (2)$$

Where, the GFF is guided filter function with source image and guidance image, epsilon $\epsilon = 0.001$ and window size $winsize = 3$.

The pre-processed image I^2 then decomposed into the different blocks and stored into the vector $B^{nonoverlap}$. On each block j, we have applied $getGIF$ (.) function to extract the 8 features. The $getGIF$ (.) function extracts the moments and invariants for each block. Moments and their invariants can be employed efficiently for invariant object identification and geometric invariant retrieval if the experimental parameters are carefully monitored.

The geometric moment features of different orders extracted from the each block image. The block j of $x - y$ plan with non-zero elements is having the moments. The geometric moment of order (p, q) for a 2DROI imageis computed as:

$$m_{pq} = \sum_{x=1}^{m} \sum_{y=1}^{n} x^p y^q j(i,j) \quad (3)$$

Geometric moments of low orders have an intuitive meaning – m_{00} is a "mass" of the each block, m_{10}/m_{00} and m_{01}/m_{00} define the centroid of each block image. Second-order moments m_{20} and m_{02}represents the "distribution of mass" of the each block with respect to the coordinate axes.In the case of geometric moments, we have central geometric moments of order (p, q):

$$\mu_{pq} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})^q j(x, \bar{y}) \quad (4)$$

Where, $\bar{x} = \frac{m_{10}}{m_{00}}$ and $\bar{y} = \frac{m_{01}}{m_{00}}$ are the coordinates of the object centroid. In this way, we have computed 8 moments as:

$$m_{00} = \sum_{x=1}^{m} \sum_{y=1}^{n} j(x,y) \quad (5)$$

$$m_{10} = \sum_{x=1}^{m} \sum_{y=1}^{n} x\, j(x,y) \quad (6)$$

$$m_{01} = \sum_{x=1}^{m} \sum_{y=1}^{n} y\, j(x,y) \quad (7)$$

$$\mu_{11} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})(y - \bar{y}) j(x,y) \quad (8)$$

$$\mu_{12} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})(y - \bar{y})^2 j(x,y) \quad (9)$$

$$\mu_{21} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})^2 (y - \bar{y}) j(x,y) \quad (10)$$

$$\mu_{30} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})^2 (y - \bar{y})^2 j(x,y) \quad (11)$$

$$\mu_{30} = \sum_{x=1}^{m} \sum_{y=1}^{n} (x - \bar{x})^3 j(x,y) \quad (12)$$

The outcome of features extracted for each block is stored in to the vector B^{GIF}. After that, we have sorted the vector B^{GIF} lexically into the another vector B^{sort}. As showing in algorithm 1, we have conducted the similarity checking among two sorted blocks to extract the candidate blocks using the pre-defined threshold value (T1). The candidate blocks are stored into vector CB. Finally, the forgery blocks are detected using another pre-defined threshold value (T2). If any block is detected forgery, we marked it by black color (by setting the pixels value 0) on the input digital image. Further, we have applied the simple steps of localizing the forgery blocks. Figure 2 and 3 shows the examples of forgery localization.

Figure 2. Forgery Detection And Localization Example 1

Figure 3. Forgery Detection And Localization Example 2

4. Simulation Results

This section discusses the Simulation Results of the Proposed Technique using several Forgery Datasets. Using the MATLAB tool, the recommended Copy-Move Forgery Detection Techniques were developed on Windows 10 with 4 GB RAM and an Intel I3 CPU. Rather than conducting a comparison analysis with similar methodologies, we concentrated on evaluating the suggested methodology using Different Datasets with block sizes ranging from 5 to 20. The suggested technique was tested utilising datasets such as MICC-F220 [35], MICC-F2000 [35], MICC-F8multi [35], and Comofod [46].

We have compared the Performance of the Proposed model with three recent similar methods such as Vega et al. [12], Bilal et al. [19], and Priyanka et al. [13]. The Performances are measured in terms of Hit Rate (HR), Miss Rate (MR), False Detection Rate (FDR), and execution time.

$$HR = \left(\frac{Number\ of\ forged\ images\ detected\ as\ forged}{Total\ number\ of\ forged\ images}\right) \times 100 \quad (13)$$

$$MR = \left(\frac{Number\ of\ forged\ images\ detected\ as\ not\ forged}{Total\ number\ of\ forged\ images}\right) \times 100 \quad (14)$$

$$FDR = \left(\frac{Number\ of\ original\ images\ detected\ as\ forged}{Total\ number\ of\ original\ images}\right) \times 100 \quad (15)$$

$$\text{Execution Time} = [\text{Detection Time} - \text{Image Acquisition time}] \quad (16)$$

Figures 4-7 demonstrates the Simulation Results using each dataset for each method in terms of Hit Rate, Miss Rate, False Detection Rate, and Execution Time respectively. The Hit Rate Performance of the Proposed SWT-SVD method as shown Figure 4 proves the efficiency of the proposed SWT-SVD approach for the correct forgery detection compared to existing methods.

The key reasons behind such improvement are the block-based Geometric Invariant Features connected with Guided Filtering for the image quality improvement. The performance of the Hit Rate has directly effect on the other performances of other parameters such as Miss Rate (Figure 5) and False Detection Rate
(Figure 6).

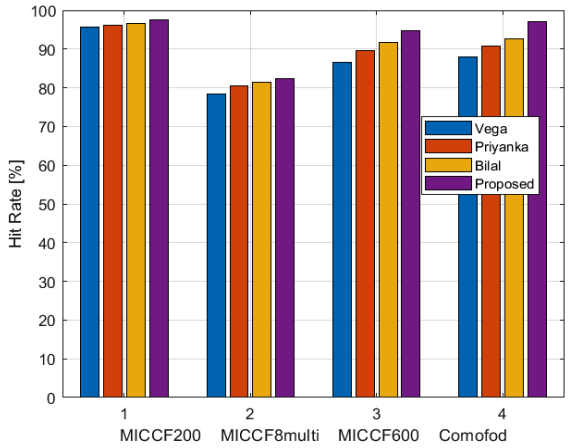

Figure 4. Hit Rate Performance Analysis

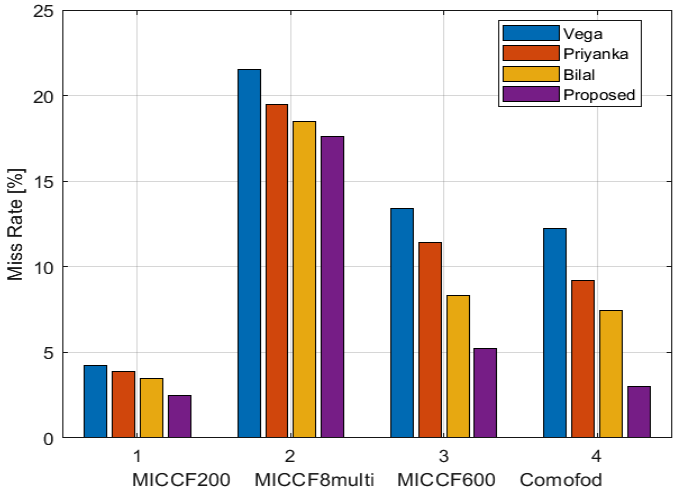

Figure 5. Miss Rate Performance Analysis

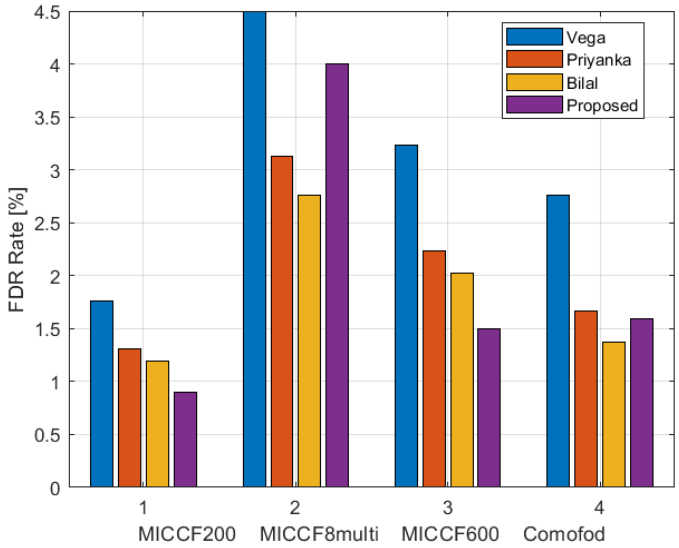

Figure 6. False Detection Rate Performance Analysis

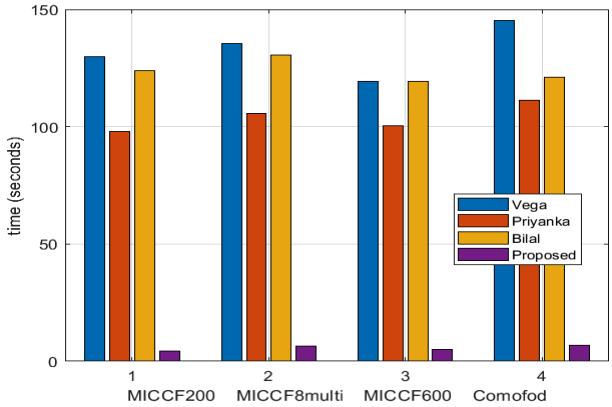

Figure 7. Execution Time Performance Analysis

The Performance of the Forgery Detection Execution Time parameter displaying in Figure 7 reflects that proposed model reduced the execution time required for the forgery detection significantly compared to other similar methods. Table 1 shows the Average Performances of each method. In the proposed model, we have set block size to 10x10. The Average Results in Table 1 proves that proposed model achieved efficiency and robustness performance trade-off compared to all methods.

Table 1. Average Performance Analysis

Methods	**HR (%)**	**MR (%)**	**FDR (%)**	**Execution Time (Seconds)**
Vega [12]	94.5	5.5	3.5	134.77
Bilal [19]	96.8	3.2	2.2	89.83
Priyanka [13]	95.6	4.4	2.7	124.39
Proposed	**98.5**	**1.5**	**1.75**	**2.78**

5. Conclusion and Future Work

To improve fraud detection performance and total execution time, this research suggested a unique technique for copy-move forgery detection. The suggested method was unique in that it combined picture quality improvement with effective feature extraction for accurate forgery block detection. The purpose of the guided filtering was to increase the image quality. The pre-processed picture had been divided into non-overlapping blocks of various sizes. From each block, we retrieved the eight geometric invariant characteristics. Using Euclidean distance, these traits were used to detect the forged block. If any forgery blocks detected, we performed the forgery localization in this paper. Using various datasets, the simulation results explored the effectiveness and resilience of the proposed approach compared to state-of-art methods. Employing the advance techniques like deep learning for the forgery detection and localization will be the interesting future direction.

References

[1] Armas Vega, E.A., GonzlezFernndez, E., Sandoval Orozco, A.L. et al. Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Comput&Applic 33, 47134727 (2021).https://doi.org/10.1007/s00521-020-05433-1.

[2] Kharanghar M., Doegar A. (2021) Copy-Move Forgery Detection Methods: A Critique. In: Goar V., Kuri M., Kumar R., Senjyu T. (eds) Advances in Information Communication Technology and Computing. Lecture Notes in Networks and Systems, vol 135. Springer, Singapore.https://doi.org/10.1007/978-981-15-5421-6_49.

[3] Abhishek, Jindal, N. Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation. *Multimed Tools Appl***80,** 3571–3599 (2021).https://doi.org/10.1007/s11042-020-09816-3.

[4] Rodriguez-Ortega, Y., Ballesteros, D. M., &Renza, D. (2021). Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. *Journal of imaging*, *7*(3), 59.https://doi.org/10.3390/jimaging7030059.

[5] Rani A., Jain A. (2021) Digital Image Forensics-Image Verification Techniques. In: Dash S.S., Das S., Panigrahi B.K. (eds) Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 1172.Springer, Singapore.https://doi.org/10.1007/978-981-15-5566-4_19.

[6] Tahaoglu, G., Ulutas, G., Ustubioglu, B. et al. Improved copy move forgery detection method via L*a*b* color space and enhanced localization technique. Multimed Tools Appl 80, 2341923456 (2021).https://doi.org/10.1007/s11042-020-10241-9.

[7] Abhishek, Jindal, N. Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation. Multimed Tools Appl 80, 35713599 (2021).

[8] P. Kale, V. A. More and U. Shinde, Copy Move Forgery Detection-A Robust Technique, 2021 Sixth International Conference on Image Information Processing (ICIIP), 2021, pp. 121-125, doi: 10.1109/ICIIP53038.2021.9702623.

[9] Tahaoglu, G., Ulutas, G., Ustubioglu, B. *et al.* Improved copy move forgery detection method via L*a*b* color space and enhanced localization technique. *Multimed Tools Appl***80,** 23419–23456 (2021).https://doi.org/10.1007/s11042-020-10241-9.

[10] Kaur, H., Jindal, N. Image and Video Forensics: A Critical Survey. *Wireless PersCommun***112,** 1281–1302 (2020). https://doi.org/10.1007/s11277-020-07102-x

[11] Park, J. Y., Kang, T. A., Moon, Y. H., &Eom, I. K. (2020).Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram.*Symmetry*, *12*(4), 492.doi:10.3390/sym12040492

[12] Armas Vega, E. A., González Fernández, E., Sandoval Orozco, A. L., &GarcíaVillalba, L. J. (2020). Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Computing and Applications.doi:10.1007/s00521-020-05433-1.

[13] Nouby M. Ghazaly, M. M. A. . (2022). A Review on Engine Fault Diagnosis through Vibration Analysis . International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(2), 01–06. https://doi.org/10.17762/ijrmee.v9i2.364

[14] Priyanka, Singh, G., & Singh, K. (2020). An improved block based copy-move forgery detection technique. Multimedia Tools and Applications.doi:10.1007/s11042-019-08354-x.

[15] Wang, XY., Wang, C., Wang, L. et al. A fast and high accurate image copy-move forgery detection approach.MultidimSyst Sign Process 31, 857883 (2020).https://doi.org/10.1007/s11045-019-00688-x.

[16] Park, J. Y., Kang, T. A., Moon, Y. H., &Eom, I. K. (2020). Copy-Move Forgery Detection Using Scale Invariant Feature and Reduced Local Binary Pattern Histogram.Symmetry, 12(4), 492.doi:10.3390/sym12040492.

[17] Ms.Preeti Kale, Dr.Vijayshree A. More, Dr.ShindeUlhas,Comparison of Copy Move Forgery Detection Algorithms both Between DWT and SWT ,International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-06, Issue-04, July 2020

[18] Ms.Preeti Kale, Dr.Vijayshree A. More, Dr.ShindeUlhas, Comparison of Copy Move Forgery Detection Algorithms both Between DWT and SWT, International Journal for Research in Engineering Application & Management (IJREAM)ISSN : 2454-9150 Vol-06, Issue-04, July 2020.

[19] Alaria, S. K., A. . Raj, V. Sharma, and V. Kumar. "Simulation and Analysis of Hand Gesture Recognition for Indian Sign Language Using CNN". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 10-14, doi:10.17762/ijritcc.v10i4.5556.

[20] Meena K.B., Tyagi V. (2019) Image Forgery Detection: Survey and Future Directions. In: Shukla R.K., Agrawal J., Sharma S., Singh Tomer G. (eds) Data, Engineering and Applications. Springer, Singapore.https://doi.org/10.1007/978-981-13-6351-1 14.

[21] Bilal, M., Habib, H. A., Mehmood, Z., Saba, T., & Rashid, M. (2019). Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering. Arabian Journal for Science and Engineering.doi:10.1007/s13369-019-04238-2.

[22] Ms.Preeti Kale, Dr.Vijayshree A. More, Dr.ShindeUlhas, A Passive Technique based on CWT FFT forRegion Duplication Detection in Digital Images, International Journal for Research in Engineering Application & Management (IJREAM) ISSN : 2454-9150 Vol-05, Issue-03, June 2019

[23] Raju, Priya& S. Nair, Madhu. (2018). Copy-move forgery detection using binary discriminant features. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2018.11.004.

[24] Sun, Yu & Ni, Rongrong& Zhao, Yao. (2018). Nonoverlapping Blocks Based Copy-Move Forgery Detection. Security and Communication Networks. 2018. 1-11. 10.1155/2018/1301290.

[25] Philip, A. M., and D. S. . Hemalatha. "Identifying Arrhythmias Based on ECG Classification Using Enhanced-PCA and Enhanced-SVM Methods". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 01-12, doi:10.17762/ijritcc.v10i5.5542.

[26] Sadeghi, S., Dadkhah, S., Jalab, H.A. et al. State of the art in passive digital image forgery detection: copy-move image forgery. Pattern Anal Applic 21, 291306 (2018).https://doi.org/10.1007/s10044-017-0678-8.

[27] Raju, Priya& S. Nair, Madhu. (2018). Copy-move forgery detection using binary discriminant features. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2018.11.004.

[28] Imran, Muhammad & Ali, Zulfiqar&Bakhsh, Sheikh &Akram, Sheeraz. (2017). Blind Detection of Copy-Move Forgery in Digital Audio Forensics. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2717842.

[29] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[30] Dixit, Rahul &Naskar, Ruchira& Mishra, Swati.(2017). Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD. IET Image Processing. 11. 10.1049/iet-ipr.2016.0537.

[31] Zhong, Junliu&Gan, Yanfen& Young, Janson& Huang, Lian& Lin, Peiyu.(2017). A new block-based method for copy move forgery detection under image geometric transforms.Multimedia Tools and Applications. 76. 10.1007/s11042-016-4201-9.

[32] Elaskily, M. A., Aslan, H. K., Elshakankiry, O. A., Faragallah, O. S., El-Samie, F. E. A., &Dessouky, M. M. (2017). Comparative study of copy-move forgery detection techniques. 2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT). doi:10.1109/accs-peit.2017.8303041.

[33] Imran, Muhammad & Ali, Zulfiqar&Bakhsh, Sheikh &Akram, Sheeraz. (2017). Blind Detection of Copy-Move Forgery in Digital Audio Forensics. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2717842.

[34] P. Modiya and S. Vahora, “Brain Tumor Detection Using Transfer Learning with Dimensionality Reduction Method”, Int J Intell Syst Appl Eng, vol. 10, no. 2, pp. 201–206, May 2022.

[35] Dixit, Rahul &Naskar, Ruchira& Mishra, Swati. (2017). Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD. IET Image Processing. 11. 10.1049/ietipr.2016.0537.

[36] Zhong, Junliu&Gan, Yanfen& Young, Janson& Huang, Lian& Lin, Peiyu. (2017). A new block-based method for copy move forgery detection under image geometric transforms.Multimedia Tools and Applications. 76. 10.1007/s11042-016-4201-9.

[37] Wenchang, Shi &Fei, Zhao & Bo, Qin & Bin, Liang. (2016). Improving image copy-move forgery detection with particle swarm optimization techniques. China Communications. 13. 139-149. 10.1109/CC.2016.7405711.

[38] Zandi, Mohsen &Mahmoudi-Aznaveh, Ahmad &Talebpour, Alireza. (2016). Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector.IEEE Transactions on Information Forensics and Security. 11. 2499 - 2512. 10.1109/TIFS.2016.2585118

[39] Li, Jian& Li, Xiaolong& Yang, Bin &Xingming, Sun. (2015).Segmentation-Based Image Copy-Move Forgery Detection Scheme.IEEE Transactions on Information Forensics and Security. 10. 507-518. 10.1109/TIFS.2014.2381872.

[40] http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.

[41] P. Kale and S. T. Gandhe, ”Hybrid binarization, histo-equalization: Comparison of old image enhancement techniques,” 2015 International Conference on Information Processing (ICIP), 2015, pp. 182-187, doi: 10.1109/INFOP.2015.7489374.

[42] P. Kale, G. M. Phade, S. T. Gandhe and P. A. Dhulekar, ”Enhancement of old images and documents by digital image processing techniques,” 2015 International Conference on Communication, Information & Computing Technology (ICCICT), 2015, pp. 1-5, doi: 10.1109/ICCICT.2015.7045709.

[43] Fattah, ShaikhAnowarul&Ullah, M. & Ahmed, M. &Ahmmed, I. &Shahnaz, C..(2014). A scheme for copy-move forgery detection in digital images based on 2D-DWT. Midwest Symposium on Circuits and Systems.801-804. 10.1109/MWSCAS.2014.6908536.

[44] Hashmi, M. F., Anand, V., &Keskar, A. G. (2014). Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform. AASRI Procedia, 9, 8491. doi:10.1016/j.aasri.2014.09.015.

[45] Fattah, ShaikhAnowarul&Ullah, M. & Ahmed, M. &Ahmmed, I. &Shahnaz, C..(2014). A scheme for copy-move forgery detection in digital images based on 2D-DWT. Midwest Symposium on Circuits and Systems.801-804. 10.1109/MWSCAS.2014.6908536.

[46] Raghavan, S. Digital forensic research: current state of the art. *CSIT***1,** 91–114 (2013).https://doi.org/10.1007/s40012-012-0008-7

[47] Sheng Y., Wang H., Zhang G. (2013) Comparison and Analysis of Copy-Move Forgery Detection Algorithms for Electronic Image Processing. In: Jin D., Lin S. (eds) Advances in Mechanical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 178. Springer, Berlin, Heidelberg.https://doi.org/10.1007/978-3-642-31528-2_54.

[48] Sridevi M., Mala C., Sanyam S. (2012) Comparative Study of Image Forgery and Copy-Move Techniques. In: Wyld D., Zizka J., Nagamalai D. (eds) Advances in Computer Science, Engineering & Applications. Advances in Intelligent and Soft Computing, vol 166.Springer, Berlin, Heidelberg.https://doi.org/10.1007/978-3-642-30157-5_71.

[49] Redi, J.A., Taktak, W. &Dugelay, JL. Digital image forensics: a booklet for beginners. *Multimed Tools Appl***51,** 133–162 (2011).https://doi.org/10.1007/s11042-010-0620-1.

[50] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra. A SIFTbased forensic method for copy-move attack detection and transformation recovery, IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110, 2011.

[51] https://www.vcl.fer.hr/comofod/

[52] https://doi.org/10.1007/s11042-020-09816-3.

[53] Udomhunsakul, S., &Wongsita, P. (n.d.). Feature extraction in medicalMRI images. IEEE Conference on Cybernetics and Intelligent Systems,2004.doi:10.1109/iccis.2004.1460437.