ISSN 2277-2685
IJESR/Jan-Mar. 2025/ Vol-15/Issue-1s/223-232
Sk. Sama Nehak *et. al.*, / International Journal of Engineering & Science Research

Image Copy Move Forgery Detection Based on Spatial feature Domain

[1]Ms. B Jyothsna, [2]Sk. Sama Nehak, [3]D. Swathi, [4]V.V. Praveena Kirani

[1] Associate professor, Electronics and Communication Engineering, BRECW

[2,3,4]B.Tech Students, Department of Electronics and Communication Engineering, BRECW

ABSTRACT

Copy-move forgery is a prevalent form of digital image manipulation where a segment of an image is duplicated and pasted within the same image to conceal information or create misleading content. Detecting such alterations is crucial for maintaining the integrity of digital images in fields like digital forensics, journalism, and legal investigations. This project explores spatial feature-based algorithms designed to identify copy-move forgery, highlighting the methods' key steps and unique characteristics.

Spatial feature-based detection focuses on the intrinsic properties of image pixels to identify repeated segments. The process typically involves three main stages: feature extraction, feature matching, and post-processing verification.

Feature Extraction involves extracting unique attributes from an image that can help identify duplicated sections. Techniques like SIFT, SURF and ORB are commonly used to derive these features due to their robustness and versatility. Once features are extracted, the algorithm searches for patterns of similarity within the image, which might indicate duplicated regions. This is accomplished through various methods like KD-Trees, hashing, or clustering to find sets of similar features. After identifying possible matches, the algorithm applies further analysis to confirm whether these matches indeed represent a copy-move forgery. Techniques like RANSAC (Random Sample Consensus) and geometric transformations are employed to refine and validate the results.

This project examines these algorithm's effectiveness in detecting copy-move forgeries and discusses their resilience to common manipulations such as rotation, scaling, and compression. The study also addresses the computational demands of these methods, considering their applicability in real-world scenarios. By focusing on spatial feature-based algorithms, the project provides insights into current techniques for copy-move forgery detection, highlighting areas for improvement and future research.

1-INTRODUCTION

The world is getting advanced day by day as the technology is growing rapidly. According to the type of wish he needed, human develops different software's. Hence likewise now many image editing software are available. Using these tools the images get edited. This editing may have a positive face as well as a negative face. The negative face may cause for a human life itself. Now different editing tools are available that can edit the image in any way as they wish. Many morphological operations can be occurred in an image. These manipulations in an image are a serious issue regarding the authenticity, integrity, and reliability of the image. More and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into other

part(s) of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case.

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our email in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emer`ged to help restore some trust to digital images. Here I review the state of the art in this new and exciting field. Digital watermarking has been proposed as a means by which an image can be authenticated. The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post processing.

2- LITERATURE SURVEY

Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into other part(s) of the same image. Noise addition is occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point-based algorithms. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions applied Principal Component Analysis (PCA) to reduce the feature dimensions used the RGB colour components and direction information as block

features used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features calculated the 24 Blur-invariant moments as features calculated the singular values of a reduced-rank approximation in each block used the Fourier-Mellin Transform (FMT) to obtain features used the mean intensities of circles with different radii around the block centre to represent the block features used the gray average results of each block and its sub-blocks as the block features used Zernike moments as block features used information entropy as block features. As an alternative to the block-based methods, key point-based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In the Scale-Invariant Feature Transform was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In the Speeded up Robust Features were applied to extract features instead of SIFT. However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate. Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing key point-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing key point based forgery methods were very poor.

An attempt is made to survey the recent developments in the field of digital image forgery detection. And a novel copy–move forgery detection scheme using adaptive over-segmentation and feature point matching. Also it explained the scheme integrates both block-based and key point-based forgery detection methods. The proposed adaptive over-segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, it applies the morphological operation to the merged regions to generate the detected forgery regions described to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point-based algorithms. This work comes under block-based forgery detection methods. The existing block-based forgery

detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. And proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions.

For a Method Image features in an image can be added up or removed, without leaving any obvious traces in the image. Thus the method called forensic detection is used to detect such manipulations occurred in an image by recovering the history of an image. Here recovers the history of filtered JPEG image using an effective linear classifier that discriminates the forensic image with its trained data. Copy- move forgery is a type of image forgery where a portion of image gets copied and pasted at another location of the same image, which cannot be detected by naked eye. The method to detect such forgery is to initially segment the image using adaptive block segmentation and features are extracted from each image blocks and compare each blocks to one another to found out the match. Label the matched points to extract the forged region. Hence forged region is detected. The image tampering includes both splicing and copy-move forgery. First, the image was decomposed into three color channels (one luminance and two Chroma), and each channel was divided into non overlapping blocks. Local textures in the form of local binary pattern (LBP) were extracted from each block. The histograms of the patterns of all the blocks were concatenated to form a feature vector. The feature vector was then fed to an ELM for classification. The ELM is a powerful and fast classification approach. The experiment was performed using two publicly available databases. The experimental results showed that the proposed method achieved high detection accuracy in both the databases.

3- REVIEW OF EXISTING AND PROPOSED SYSTEMS

In this chapter we will discuss about Existing/Proposed System of Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain.

Existing System

Pixel based Feature Transform for Copy-Move Forgery Detection

As noted above, many methods of detecting CMF have been suggested. Christlein et al, tested the 15 most prominent feature sets by creating a real-world copy-move dataset and a software framework for systematic image manipulation. They analysed the performance of the detection on a per-pixel basis and a per-image basis. In their experiments, SIFT and SURF keypoint-based feature worked very well in detection CMF, and so did block-based DCT, DWT, kernel PCA, PCA and Zernike moments.

According to Christlein et al, the Zernike moments achieved the most precise detection results (state of the art). Therefore, we compared our improved DSIFT with Zernike moments to see which produced better results.

One of our contributions is to have combined ideas derived from the keypoint and block-based methods. We chose the Scale Invariant Feature Transform (SIFT) method and applied it densely to make block-based matching possible. SIFT is the most widely used descriptor; it is distinctive and relatively fast. However, in some cases, the high dimensionality of the descriptor is considered a

drawback in the matching step. The other main contributions are improved the DSIFT and developed the automatic similarity thresholding.

Proposed system

Adaptive Over-Segmentation

The proposed image forgery detection using adaptive over-segmentation in details. Figure shows the framework of the proposed scheme for image forgery detection. Firstly, the adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks. Then SLIC is applied into each block to extract feature points as block features which are matched with each other to locate the points which can approximately indicate the suspected forgery regions. Finally, the forgery regions are detected according to the matched feature points. In order to divide the host image into non-overlapping regions of irregular shape, we employ the SLIC algorithm to segment the host image into meaningful superpixels. As a non-overlapping segmentation method, SLIC can decrease the computational expenses comparing with the overlapping blocking; furthermore, in most of the cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the superpixels in SLIC is hard to decide. When the initial size is too small, it will cause large computation expenses; otherwise, when it is too large, it will cause the forgery detection results not accurate enough. At present, there is no such a good method to determine the initial size in superpixel segmentation algorithms. Therefore, in this project, we proposed the Adaptive Over-Segmentation method which can determine the initial size adaptively based on the texture of the host image and thus can divide the host image into irregular and non-overlapping blocks. In the proposed Adaptive Over-Segmentation method, firstly, the Discrete Wavelet Transform (DWT)is employed into the host image to generate the low frequency and high frequency sub-bands. Then the initial size of the super-pixels is calculated with the adaptive block size computation. Finally, with the calculated initial size, the SLIC segmentation algorithm is employed to segment the host image into irregular and non-overlapping image blocks.

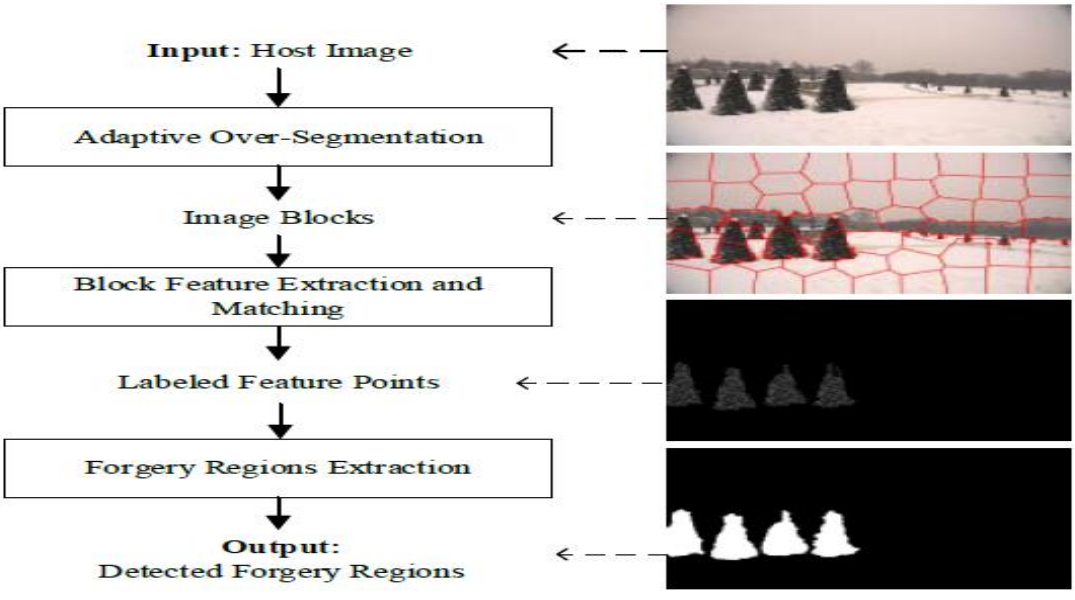

Figure 2.1 Block Diagram of Image CFMD

4-EFFICIENT DETECTION OF IMAGE TAMPERING

This chapter explores advanced techniques for detecting copy-move forgery in images, focusing on feature extraction, key point matching, and innovative algorithms to enhance accuracy and efficiency in forgery identification.

Algorithms for Efficient Forgery Detection

Copy-move forgery involves duplicating a segment of an image and pasting it elsewhere within the same image. This results in a correlation between the original and pasted regions, forming the basis for detecting this type of forgery. Due to potential compression in the lossy JPEG format or localized image processing tools like retouching, exact matches between segments may not be present, necessitating the development of detection algorithms that allow for approximate matches.

The detection algorithm must meet three key requirements:

1. Allow for approximate matching of small image segments.
2. Operate within a reasonable time frame, minimizing false positives.
3. Detect forgeries involving connected components rather than random small patches or pixels.

Two algorithms for detecting copy-move forgery are introduced: one based on exact matches and another on approximate matches. Before focusing on the more efficient block matching approach, two simpler but less practical methods were explored: Exhaustive search and Autocorrelation.

Exhaustive search is conceptually straightforward and involves overlaying an image and its circularly shifted version to find matching segments. For example, if x_{ij} represents the pixel value at position i, j in a grayscale image of size $M \times N$, the exhaustive search compares all pixel values with those in the shifted version of the image. The differences between corresponding pixels $| x_{ij} - x_{i+k \bmod(M), j+l \bmod(N)} |$ are computed for all shifts k and l, where $1 \leq k \leq M/2$ and $1 \leq l \leq N/2$. This reduces computational complexity by a factor of four, but the approach remains computationally expensive.

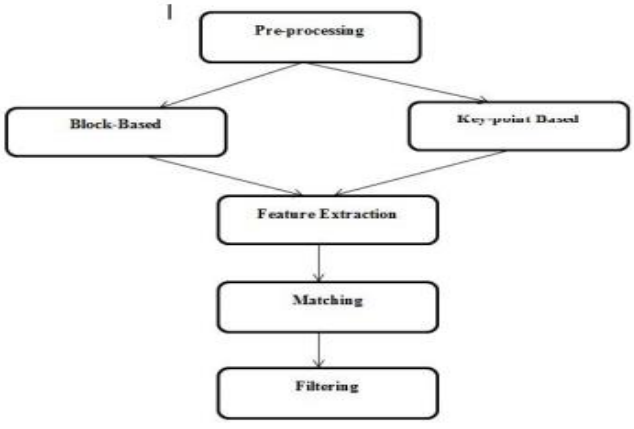

Figure 3.3 Image Tampering Detection Process Flow

5-ADVANTAGES, DISADVANTAGES AND APPLICATIONS

Advantages

- BLUR invariants don't get affected by blur degradation and additive noise.
- Robust against blurring and lossy JPEG compression.
- Efficient detection of flat copied regions.
- Small variations due to noise and lossy compression can be detected accurately.
- Less computation complexity and robust against post processing operations.
- Forgeries with additive noise and JPEG compression can be detected.

Disadvantages

- For low quality image, as size of block decreases so does efficiency
- Unable to detect forgeries with scaling and heavy JPEG compression.
- These algorithms can be affected by noise in the image, which may lead to false positives or negatives in forgery detection.
- Algorithms may struggle with more sophisticated forgery techniques that involve multiple alterations or blending, making detection less reliable.

Applications

The detection of image manipulation is very important because an image can be used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image.

- Used by law enforcement and forensic analysts to verify the authenticity of images in criminal investigations, ensuring that evidence presented in court is not tampered with.
- Helps journalists and media organizations verify the integrity of images used in news reporting, combating misinformation and maintaining credibility.
- Employed by platforms to detect manipulated images that can spread misinformation, disinformation, or harmful content.

6-SOFTWARE REQUIREMENTS

In this chapter we will discuss and software requirements for Image copy move forgery detection based on spatial feature domain.

MATLAB

What is MATLAB? Programming assignments in this course will almost exclusively be performed in MATLAB, a widely used environment for technical computing with a focus on matrix operations. The name MATLAB stands for "Matrix Laboratory" and was originally designed as a tool for doing numerical computations with matrices and vectors. It has since grown into a high-performance language for technical computing. MATLAB integrates computation, visualization, and programming in an easy-to-use environment, and allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages. Typical areas of use include:

- Math and Computation
- Modeling and Simulation
- Data Analysis and Visualization
- Application Development
- Graphical User Interface Development 1.2 Getting Started Window Layout The first timeyou start

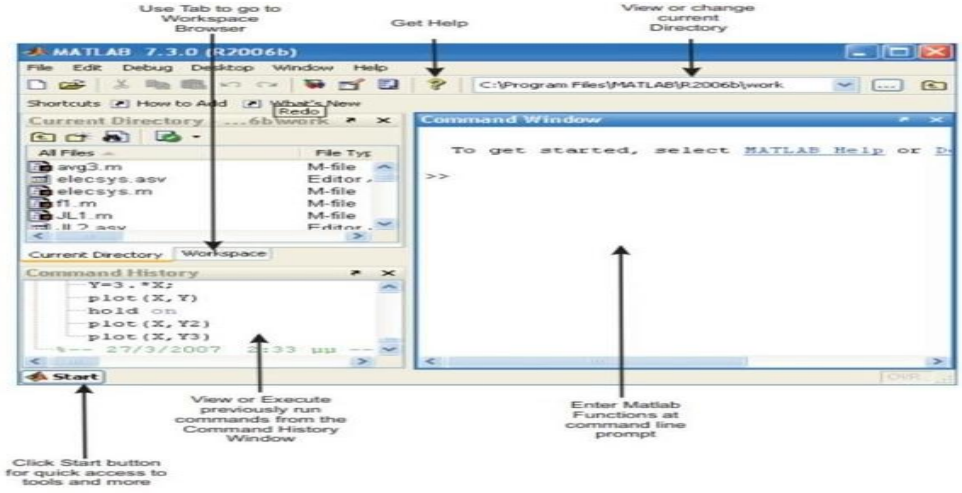

Figure 2.1: MATLAB Desktop (default layout)

7-RESULTS AND DISCUSSION

In this chapter, we will discuss about the results of the Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain

The dataset is formed based on 48 high-resolution uncompressed PNG true color images. In the dataset, the copied regions are of categories of living, nature, man-made and even mixed, and they range from overly smooth to highly texture; the copy-move forgeries are created by copying, scaling and rotating semantically meaningful image regions.

Fig. shows the copy-move forgery detection results of the proposed scheme. In the first column shows the forged images selected from the dataset; the second column shows the corresponding ground truth forged regions; and the third column shows the detected forgery regions. It can be easily seen that the proposed scheme can detect the forged regions very well.

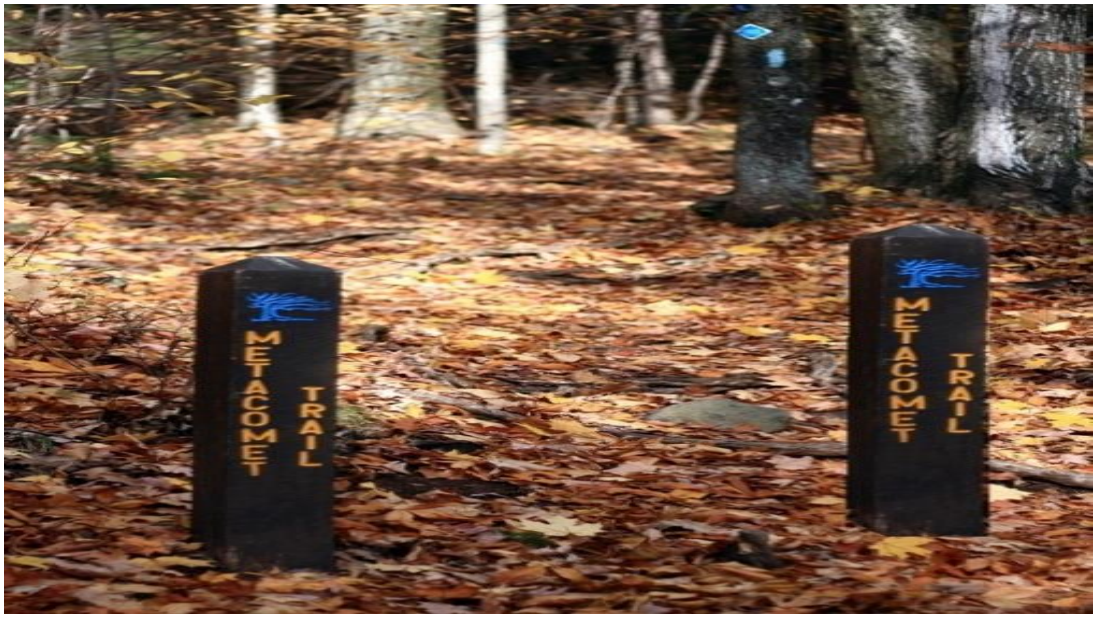

Figure 6.1 Sample Input Image

In order to evaluate the performance of the proposed scheme, the *precision* and *recall* are calculated. We also give the *F*score, which is defined as a measure which combines the *precision* and *recall* in a single value.

$$precision = \frac{\left|R \cap R'\right|}{\left|R\right|}, \qquad recall = \frac{\left|R \cap R'\right|}{\left|R'\right|}$$

Where means the set of forgery regions detected by the proposed scheme for the dataset; and means the set of all forgery regions for the dataset *R* '*R* D

$$F = 2 \times \frac{precision \times recall}{precison + recall}$$

We evaluate the proposed scheme under different conditions shows the results at both image level and pixel level, under plain copy-move, which means the one to one copy-move. Fig shows the *F* scores when the copied regions are attacked by various attacks: (a) down-Sampling, the host images are scaled down from 90% to 10% in step of 20%;(b) scaling, the copied regions are scaled with the scale factor varies from 91% to 109%, in step of 2%;(c) rotation, the copied regions are rotated with the rotation angle varies from 2º to 10º, in step of 2º; and (d) JPEG compression, the forgery images are JPEG compressed with the qualify factor varies from 100 to 20, in step of -10. It can be easily seen that in most of the cases, the proposed scheme performs much better than the existing state-of-the-art forgery detection methods.

Figure 6.2 Output Image

The output image represents the result of copy-move forgery detection using spatial feature domain techniques, where white regions indicate potential forgery or copied segments. In copy-move forgery, a portion of the image is copied and pasted elsewhere within the same image to conceal or replicate details. Spatial domain methods detect such tampering by analyzing the pixel-level features, such as intensity and texture, comparing regions to identify identical or near-identical blocks. The detection process typically involves dividing the image into overlapping blocks, followed by feature extraction (e.g., DCT, PCA, or SIFT). The system then identifies matching blocks, indicating forgery. The visual result highlights the suspicious areas, in this case, the white areas in contrast to the black background, showing regions that are likely to be duplicated and manipulated.

8-CONCLUSION

The proposed IC-MFD consists of five steps: image pre-processing, dividing the image into overlapping blocks, determining the statistical features mean and standard deviation of each block, sorting the feature into a matrix, then feeding the feature vector to the SVM classifier to classify the image as authentic or forged. Our experimental findings show that copy-move forgery can be successfully detected by the proposed IC-MFDs with high accuracy (98.44 %). We compared the results of our proposed ICMFD with many current CMFD methods. The findings revealed that our proposed produces higher outcomes than others. We plan to expand the application of our proposed in the future to distinguish other kinds of image forgeries, such as splicing.

REFERENCES

[1] M. A. Qureshi and M. Deriche, “A bibliography of pixel-based blind image forgery detection techniques,” Signal Process. Image Commun., vol. 39, pp. 46–74, 2015.

[2] K. Hayat and T. Qazi, “Forgery detection in digital images via discrete wavelet and discrete cosine transforms,” Comput. Electr. Eng., vol. 62, pp. 448–458, 2017.

[3] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, “A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform,” J. Vis. Commun. Image Represent., vol. 53, pp. 202–214, 2018.

[4] K. B. Meena and V. Tyagi, “A copy-move image forgery detection technique based on tetrolet transform,” J. Inf. Secur. Appl., vol. 52, p. 102481, 2020.

[5] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, “Copy move image forgery detection using Hessian and center symmetric local binary pattern,” in 2015 IEEE Conference on Open Systems (ICOS), 2015, pp. 7–11.

[6] G. Ulutas and G. Muzaffer, “A new copy move forgery detection method resistant to object removal with uniform background forgery,” Math. Probl. Eng., vol. 2016, 2016.

[7] F. Yang, J. Li, W. Lu, and J. Weng, “Copy-move forgery detection based on hybrid features,” Eng. Appl. Artif. Intell., vol. 59, pp. 73–83, 2017.

[8] P. M. Raju and M. S. Nair, “Copy-move forgery detection using binary discriminant features,” J. King Saud Univ.Inf.Sci.