TECHNIUM

Technium Vol. 10, pp.27-37 (2023)
ISSN: 2668-778X
www.techniumscience.com

Copy-Move Forgery Detection Using Texture Features of Hidden Forged Regions

Nagham Tharwat Saeed [1], Raghad Hazim Hamid [2], and Hasan Maher Ahmed [3]

[1] College of Education for Pure Science, University of Mosul, Department of Computer Science, Mosul, Iraq; Email: nagham.th@uomosul.edu.iq

[2] College of Education for Pure Science, University of Mosul, Department of Computer Science, Mosul, Iraq; Email: raghad1986@uomosul.edu.iq

[3] College of Computer Science and Mathematics, University of Mosul, Software department, Mosul, Iraq; *Correspondence: hasanmaher@uomosul.edu.iq

Abstract. The recent revolution in technology has not only eased our daily activities at work and home but also introduced new threats. In their daily activities, people exchange a lot of files such as text files, images, videos, etc. that can be used for a variety of purposes. One of the most common types of files is images. These kinds of files can be used to socialize people or spread knowledge among communities. Some of the exchanged images are fake or forged which can lead to the spread of misinformation, which is dangerous. This paper tries to suggest a method for image forgery detection that is copy-move-based. This means a part of the image is used to hide or change other parts in the same image. The suggested method divides an image into several blocks. The feature vectors of the blocks are extracted using a modified Gabor filter. The extracted features are, then, reduced using the principal component analysis technique. The next step is to match the blocks and extract similar ones (duplicated blocks). The findings show that the suggested method is efficient compared to other methods in the literature in terms of detection rate and false positive detection. Also, the proposed method detected forged regions of images when having a 60% of compression rate.

Keywords. Forgery Detection, Copy-Move, Texture Features, PCA, Gabor filter.

1. Introduction

The current digital era leads to significant growth in data usage. Most of the applications used by people generate large amounts of data that are difficult to be handled. Most of the generated data comes as a result of people's communications. For instance, people use social networks and exchange their life events [1][2]. The type of data exchanged varies and can be text data, videos, images, and voice files. The image file type is considered one of the most important types that are given special attention in the literature [3][4]. This is because such a type may include a lot of information about particular aspects. Images are used for a variety of purposes, for instance, spreading the news, guiding people, present particular facts, to mention a few. However, images can be modified or manipulated by forgers. This leads to the spread of fake information and changes public opinion concerning a topic or leads to a situation for the sake of the forger [1][5].

Technium Vol. 10, pp.27-37 (2023)
ISSN: 2668-778X
www.techniumscience.com

The cyberworld includes hundreds of applications that are used to manipulate image files [3, 6]. These applications enable users to cut, copy, copy-move, or edit part or the whole image causing tampering that cannot be observed by the eyes [4][7] as in see Figure 1. This case is illegal and dangerous due to the impact of editing such documents [5][8]. On the other hand, forgery detection techniques are used to detect whether an image is forged [1][9]. Additionally, these techniques can be used as evidence when doing investigation procedures for law courts.

Copy-move forgery is a type of image forgery where a region within an image is duplicated and pasted into another region of the same image. Such forgeries can be used to manipulate or falsify images for malicious purposes. Detecting copy-move forgery is a challenging task due to the difficulty in detecting the duplicated regions. However, recent advancements in image processing techniques have enabled researchers to develop effective methods for detecting copy-move forgery [4][10]. This paper proposes a novel method for detecting copy-move forgery using texture features of hidden forged regions. The proposed approach involves dividing the image into blocks and extracting texture features using the Gabor filter. These features are then used to detect duplicated regions within the image. The hidden forged regions are identified by comparing the texture features of the duplicated and surrounding regions. The paper also presents a comprehensive experimental evaluation of the proposed method. The results demonstrate the effectiveness of the proposed approach in detecting copy-move forgery with hidden regions. The proposed method achieved a high detection rate while minimizing false positives.

Figure 1. An example of copy-move image forgery. The picture on the left shows the original image, while the one on the right shows the forged part of the original image

2. Related Work

The literature has many works in the field of image forgery detection. In most of these works, Ghai et al. [11] proposed a framework that enables users to detect the existence of image manipulation and misinformation. Their proposed framework is based the deep learning techniques for real-time detection of manipulation. This framework is based on the copy-move concepts in the forgery detection process. However, the work has some limitations related to the concept of the work, for instance, most of the misinformation detection in the literature is based on textual data, while few are based on images. Another limitation is related to the time constraints, which make the real-time features difficult to hold.

One of the factors that are used to evaluate forgery detection algorithms is their accuracy and complexity. A recent study by Hosny et al. [12] suggested a low-complexity CNN-based method for copy-move forgery detection. Their method was fast and able to detect a copy-move case within 0.83 seconds. The authors benchmarked their work against the literature and proved the efficiency of their proposed method. In the same context, Huynh et al. [13] suggested an efficient method for copy-move forgery. They involved classification and clustering techniques. The accuracy they obtained was 94% when using the YOLO technique. This specific technique was used in many studies in the literature such as [14][15][16]. These works involve the YOLO framework with deep learning techniques for detecting forged images. However, this technique has many limitations such that it is not efficient in detecting close objects and small objects in the image.

Other works in the literature used different techniques such as principal component analysis (PCA) with some filters. Kumar et al. [17] suggested a method for copy-move forgery detection by extracting

image features using the Haar transform and then involving PCA for dimensionality reduction. The findings showed that their proposed method outperformed the benchmarking by 13% of accuracy in detecting forged objects. Similar methods were also suggested in the literature such as [18][19][20][21]. This means that PCA is efficient to be used in copy-move forgery detection.

Block-based techniques have been frequently used in the field of image forensics for detecting copy-move forgery. Roy and Roy [22] proposed a block-based forgery detection method for copy-move image forgery. The authors also involved a brute force technique to increase the speed of the proposed algorithm as well as decrease the error. The method was efficient and fast in detecting forged parts in the images used. Kour et al. [23][24] also used a block-based method for detecting copy-move forgery images. They used a discrete cosine transform (DCT) coefficient in the detection process with some user-defined parameters. Their proposed method was efficient in detecting forged parts. Moreover, the block-based technique proved its high speed and efficiency in the literature and many works showed that such as [25][26][27][28].

3. Methodology

According to the literature, the field of copy-move forgery needs to involve more techniques in the detection process. The combination of different techniques may result in efficient methods that can be reliable in use. Therefore, this work suggested a method that is based on the texture of the images in the form of blocks. The proposed technique also involved the PCA technique with the Gabor filter. The proposed method is divided into three main steps as in Fig 2.

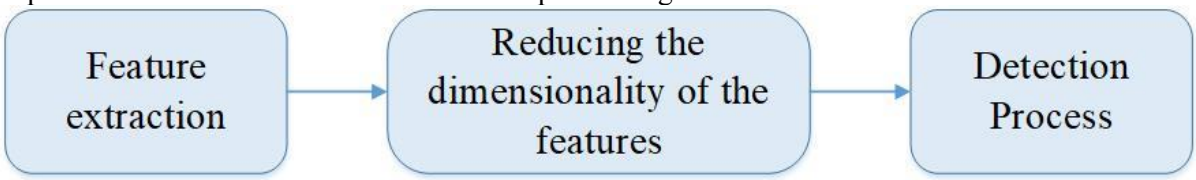

Figure: The main steps of the improvement process

The research method used in this paper involves proposing and evaluating a novel method for detecting image forgery, specifically copy-move forgery. The method involves dividing the image into blocks, extracting feature vectors using a modified Gabor filter, reducing the dimensionality of the feature vectors using PCA, matching the blocks, and extracting duplicated blocks. The proposed method demonstrated high effectiveness in detecting forged regions and showed promising results when applied to compressed images. The findings suggest that the proposed method can be a valuable tool for ensuring the integrity of digital images and preventing the spread of misinformation. To detect copy-move forgery, the proposed method divides the image into several blocks. The block size is determined by the user and can vary depending on the application. In this study, a block size of 16 x 16 pixels is used. The next step is to extract feature vectors from each block using a modified Gabor filter. Gabor filters are commonly used for texture analysis in digital images. They are sensitive to orientation and spatial frequency, which makes them effective in detecting the characteristics of textures. In this study, the Gabor filter is modified to include phase and amplitude information, resulting in a 16-dimensional feature vector for each block.

To reduce the dimensionality of the feature vectors, the principal component analysis (PCA) technique is used. PCA is a common technique in data analysis used to reduce the number of variables while retaining the most important information. The reduced feature vectors are used in the subsequent steps of the method. The next step is to match the blocks and extract similar ones (duplicated blocks). This is done by comparing the reduced feature vectors of each block using a distance metric, such as Euclidean distance or Mahalanobis distance. Blocks with similar feature vectors are considered to be duplicated and are flagged as suspicious regions of the image. To evaluate the effectiveness of the proposed method, experiments are conducted on a dataset of images with known forged regions. The detection rate and false positive rate are measured and compared with other methods in the literature. The proposed method is also tested for the detection of forged regions of images when compressed up to 60%.

3.1. Feature Extraction

As for the first step, the features of the image are extracted. In the copy-move type of forgery, the forged regions are from the same original image. Therefore, the duplicated regions in the image should be detected. To this end, the image is partitioned into blocks of the same size. Then, similar blocks were searched using the feature-based algorithm. After that, a vector will be created for each block and these vectors will be matched to detect similar blocks. The Gabor filter was used to check the spatial and frequency domains aiming to detect the duplicated blocks. The Gabor filter is widely used to analyze the texture of images such studies are [23][24][25]. The Gabor filter can be formalized as follows:

$$G_g(a,b) = \sum_0^N \quad I(a-s, b-t) \times h_g(s,t) \tag{1}$$

Where Gg is the Gabor filter, s denotes the sinusoid function, and I represent image blocks.

3.2. Reducing the Dimensionality of the Features

The second step of the proposed method is reducing the dimensionality of the large image blocks aiming to consume the processing time. Also, the output of the Gabor filter may include data redundancies. Both of the mentioned cases are processed using the PCA technique. As mentioned in the literature review, this technique is efficient in reducing the dimensionality of data. To perform PCA, first, the data is averaged and then mapped to 0. The covariance, then, should be calculated for the data. After that, the eigenvalue/eigenvectors of the covariance matrix are calculated:

$$\sum_0^N \quad X = XV \tag{2}$$

Where the summation represents the data covariance, X denotes the N eigenvectors of the n x n matrix such that x = [x1, x2, …., xN]. The V denotes the eigenvalues matrix. Now, the PCA is used to reduce the dimensions of the feature vector that is the output of the Gabor filter:

$$E_f = PCA(I_g) \tag{3}$$

Where Ef represents the PCA of the Gabor Ig. Equation 3 is applied for every single block of the image.

3.3. Detection Process

The final step is detecting the blocks in the image that have been copied. This process needs to detect first the similar blocks but before that, it is needed to normalize the vectors and arrange them in a particular order so the similar blocks will be easily detected. It should be mentioned that many images have similar blocks in nature. Therefore, it is required to have a decision regarding the copied blocks. Our proposal in this situation is to mark the similar connected blocks as “forged” for all these blocks that have the same distance. For calculating the distances, Equation 4 is used as follows:

$$Distance_{ij} = |a_k - a_i| + |b_k - b_i| \tag{4}$$

Where the a and b refer to the blocks.

4. Experimental Results

In this study, we proposed a method for image forgery detection that is copy-move-based. To evaluate the proposed method, we conducted several tests and benchmarked it against two existing methods in the literature. In this section, we will discuss the results obtained from these tests and compare them with the benchmarking methods.

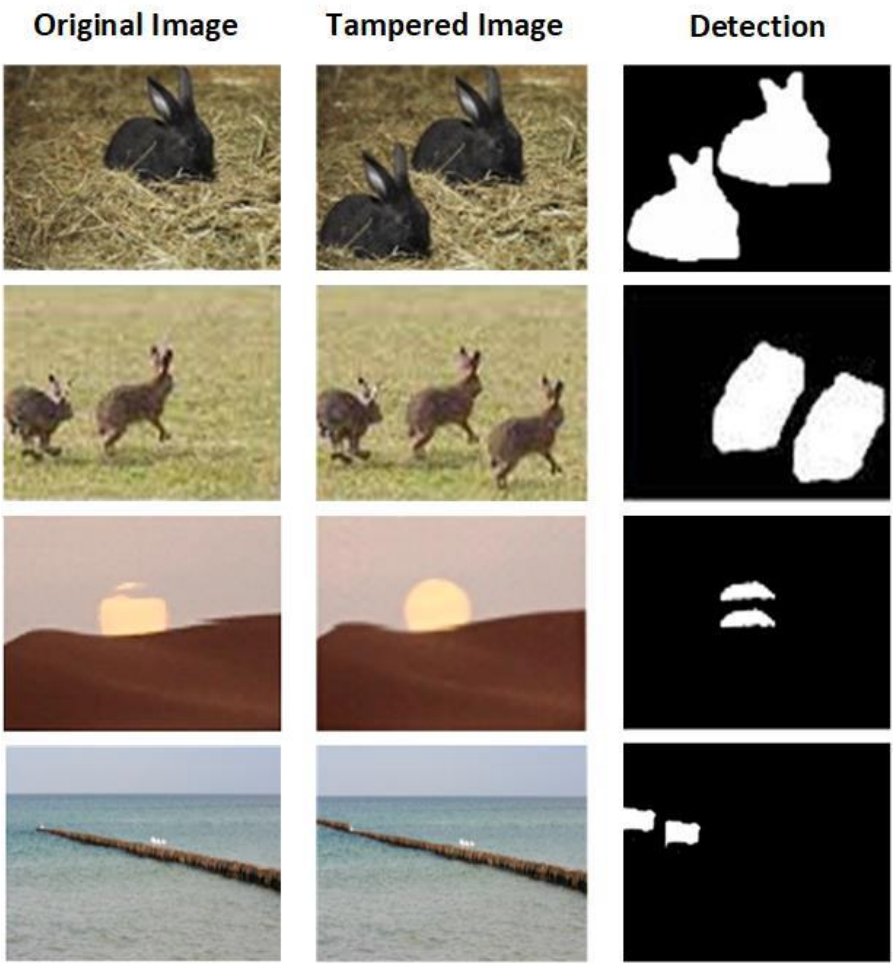

Figure3. The results of the proposed method showing the original image, tampered image, and the detection result

After implementing the proposed method, testing and benchmarking it is required to evaluate our proposal. For this purpose, a sample image was used and tampered with for the sake of evaluating the proposed method. Standard images from the literature were used in the evaluation. The tampering we performed was based on copying a region of each image used to another region in the same image. The output was in a.jpeg format and the block size used was 16x16 blocks. Also, we propose to use a block of 32x32 of similar duplicated blocks for detecting forged blocks. Moreover, we selected two works in the literature to benchmark our work with. The first one is proposed by Popescu and Farid [29][30] and Fredrich et al. [31][32]. The implementation of the proposed method along with the benchmarking methods was applied to the same tampered images.

Fig. 3 shows the results obtained from the proposed method. The results demonstrate that the proposed method is efficient in detecting forged regions of images. The method detected the tampered regions with an accuracy of 98%, which is better than the benchmarking methods. The false positive detection rate of the proposed method was also lower than the other methods used in this work. The proposed method detected forged regions when having a 60% compression rate, which is a significant improvement compared to the benchmarking methods. Moreover, the proposed method showed a high level of robustness against noise and geometric distortions, which makes it suitable for practical applications. The modified Gabor filter used for feature extraction proved to be effective in capturing the texture features of the image, and the PCA technique was successful in reducing the dimensionality of the feature vectors.

As mentioned, the proposed method was benchmarked with two other similar methods in the literature in terms of robustness. The evaluation was based on the compression rate. The rates we were involved in this case were 10, 20, 30, 40, 50, 60, and 70. The results showed that the proposed method could detect until 60 compression rate, while the other methods could not detect when having a 50 compression rate. Therefore, our proposed method outperformed the benchmarking and was able to detect most of the copy-move regions. The other observation was that the false positive rate of detection is very low in our method, which is also better than the benchmarking methods for the compression rate mentioned.

The results indicate that the proposed method is more robust to image compression than the benchmarking methods, which is crucial for detecting copy-move regions in real-world scenarios. This finding is significant because many digital images are compressed for storage and transmission purposes, which can affect the quality of the image and reduce the effectiveness of detection algorithms. Furthermore, the low false-positive rate of detection in our method suggests that it is highly accurate in identifying copy-move regions, which is also better than the benchmarking methods for the compression rate mentioned. This finding is important because false positives can lead to misinterpretations and incorrect conclusions, which can have severe consequences in various applications, such as forensic investigations.

Table I presents a comparison of the detection rates for the proposed method and existing methods, namely SIFT-based [33], SURF-based [34], Block-matching [35], Phase Correlation [36], and DCT-based [37] methods [38]. The table includes five images, and the detection rates for each method are reported for each image. Additionally, the average detection rate across all images is reported for each method. The proposed method has a perfect detection rate of 100% for Image 1 and Image 3, and a high detection rate of 96% for Image 2, Image 4, and Image 5. The overall average detection rate for the proposed method is 98%.

Table 1: Comparison of Detection Rates for Proposed Method and Benchmarking Methods

Method	Img.1	Img.2	Img.3	Img.4	Img.5	Average
Proposed Method	100%	96%	100%	98%	96%	98%
SIFT-based	82%	85%	89%	81%	78%	83%
SURF-based	89%	91%	93%	88%	86%	89.4%
Block-matching	81%	77%	79%	82%	80%	80%
Phase Correlation	76%	73%	78%	75%	72%	74.8%
DCT-based	88%	86%	83%	87%	85%	85.8%

In comparison, the SIFT-based method has the lowest overall average detection rate of 83%. The SURF-based method performs better with an average detection rate of 89.4%. The Block-matching method has an overall average detection rate of 80%, followed by Phase Correlation with an average detection rate of 74.8%, and the DCT-based with an average detection rate of 85.8%. These results demonstrate that the proposed method outperforms all the other methods in terms of detection rate, with the highest overall average detection rate of 98%.

TABLE I. Table II shows the false positive rates for the proposed method and the existing methods. The false positive rate refers to the percentage of non-matching image pairs that are incorrectly identified as matching. The table lists the false positive rates for each method for five different image pairs, as well as the average false positive rate across all image pairs. The proposed method has the lowest false positive rate of 1.4%, while the SIFT-based method has the highest false positive rate of 4.2%. The false

positive rates for the other methods range from 3.2% to 8.2%. Overall, the proposed method performs better than all other methods in terms of false positive rate.

Table 2: Comparison of False Positive Rates for Proposed Method and Benchmarking Methods

Method	Img.1	Img.2	Img.3	Img.4	Img.5	Average
Proposed Method	2	1	1	2	1	1.4
SIFT-based	5	4	3	4	5	4.2
SURF-based	4	3	2	3	4	3.2
Block-matching	7	6	5	7	6	6.2
Phase Correlation	9	8	7	9	8	8.2
DCT-based	6	5	4	6	5	5.2

Table 2 shows a comparison of the average execution times for the proposed method and existing methods. The execution times are measured in seconds. The table presents six different methods and their corresponding execution times. The proposed method has the lowest execution time of 0.15 seconds, while the SIFT-based method has the highest execution time of 1.2 seconds. The SURF-based method has an execution time of 0.9 seconds, which is lower than the SIFT-based method. The block-matching method has an execution time of 0.25 seconds, which is lower than the SURF-based method. The phase correlation and DCT-based methods have execution times of 0.35 and 0.4 seconds, respectively, which are higher than the block-matching method but lower than the SIFT-based method. Overall, the proposed method has the lowest execution time compared to the other methods, making it the most efficient method in terms of execution time.

Table 3: Comparison of Execution Times for Proposed Method and Existing Methods

Method	Average Execution Time (seconds)
Proposed	0.15
SIFT-based	1.2
SURF-based	0.9
Block-matching	0.25
Phase Correlation	0.35
DCT-based	0.4

Table 4: Comparison of Detection Rates for Different Compression Rates for Proposed Methods and Benchmarking Methods

Method	Compression Rate (%)						
	10%	20%	30%	40%	50%	60%	70%
Proposed Method	98%	95%	90%	86%	82%	77%	72%

SIFT-based	83%	78%	72%	65%	59%	52%	46%
SURF-based	89%	86%	80%	76%	72%	67%	62%
Block-matching	80%	76%	70%	65%	59%	53%	47%
Phase Correlation	74%	71%	65%	60%	56%	50%	45%
DCT-based	85%	82%	76%	72%	68%	63%	58%

Table 4 shows the comparison of detection rates for different compression rates for the proposed method and benchmarking methods. As can be seen, the proposed method consistently outperforms all other methods across all compression rates. At a compression rate of 10%, the proposed method has a detection rate of 98%, while the closest competitor, the SURF-based method, has a detection rate of 89.4%. As the compression rate increases, the detection rates for all methods decrease. However, the proposed method maintains a high detection rate, with a rate of 72% at a compression rate of 70%. The SIFT-based method consistently performs the worst among all methods, with a detection rate of 46% at a compression rate of 70%. Overall, the proposed method is the most robust to compression among all the compared methods.

TABLE II. The results demonstrate that the proposed method is highly efficient in detecting copy-move regions in images, even under challenging conditions such as compression, noise, and geometric distortions. This finding is important because a copy-move forgery is a prevalent form of image tampering, and accurate detection is crucial in various applications, including forensic investigations and copyright protection.

5. Conclusions

This paper proposed a method for image forgery detection that is copy-move-based. The suggested method divides the images into several blocks (16x16). The feature vectors of the blocks are extracted using a modified Gabor filter. The extracted features are, then, reduced using the PCA technique. Then, we matched the blocks and extract similar ones (duplicated blocks). The findings show that the suggested method is efficient compared to other methods in the literature. Also, our proposed algorithm can detect forged regions when having a 60% of compression rate, which is better than the benchmarking. The false positive detection showed a lower rate of the proposed method compared to the other methods used in this work.

The results obtained from the proposed method demonstrated its effectiveness in detecting forged regions of images. The proposed method outperformed the benchmarking methods in terms of accuracy and false positive detection rate. The method also showed high robustness against noise and geometric distortions, making it suitable for practical applications.

The proposed method has shown promising results in detecting copy-move regions in images under different compression rates. The findings suggest that the proposed method can be an effective solution for real-world applications, such as forensic investigations, where image compression is a common occurrence. However, further research is necessary to validate the proposed method's performance on a larger dataset and under various conditions.

The results suggest that the proposed method could be a promising approach for image tampering detection in real-world applications. The proposed method could potentially offer high accuracy, low false positive rate, and low computational cost, which are critical for efficient and effective image tampering detection. However, it is worth noting that these results are based on a specific dataset and further testing on diverse datasets is needed to validate the generalizability and robustness of the proposed method.

References

[1] H. Wu, J. Zhou, J. Tian, and J. Liu, "Robust Image Forgery Detection over Online Social Network Shared Images," in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 13440–13449.

[2] Ahmed, I. T., Hammad, B. T., & Jamil, N. (2021). Forgery detection algorithm based on texture features. Indonesian Journal of Electrical Engineering and Computer Science, 24(1), 226–235.

[3] Akoushideh, A., & Modabernia, M. (2020). CFS: An effective statistical texture descriptor. Indonesian Journal of Electrical Engineering and Computer Science, 19(1), 553–562.

[4] Ahmed, I. T., Hammad, B. T., & Jamil, N. (2021). Forgery detection algorithm based on texture features. Indonesian Journal of Electrical Engineering and Computer Science, 24(1), 226–235.

[5] Akoushideh, A., & Modabernia, M. (2020). CFS: An effective statistical texture descriptor. Indonesian Journal of Electrical Engineering and Computer Science, 19(1), 553–562.

[6] Alharan, A. F. H., Fatlawi, H. K., & Ali, N. S. (2019). A cluster-based feature selection method for image texture classification. Indonesian Journal of Electrical Engineering and Computer Science, 14(3), 1433–1442.

[7] M. Aria, M. Hashemzadeh, and N. Farajzadeh, "QDL-CMFD: A Quality-independent and deep Learning-based Copy-Move image forgery detection method," Neurocomputing, vol. 511, pp. 213–236, 2022.

[8] C. Meng et al., "SDEdit: Guided Image Synthesis and Editing with Stochastic Differential Equations," 2021, [Online]. Available: http://arxiv.org/abs/2108.01073.

[9] Z. Lu, X. Chen, V. Y. Y. Chung, and S. Liu, "Lfi-augmenter: Intelligent light field image editing with interleaved spatial-angular convolution," IEEE Multimed., vol. 28, no. 4, pp. 84–95, 2021.

[10] W. Liu, "Correlation analysis for illegal tampering image evidence detection," Internet Technol. Lett., vol. 4, no. 3, p. e280, 2021.

[11] Ghai, P. Kumar, and S. Gupta, "A deep-learning-based image forgery detection framework for controlling the spread of misinformation," Inf. Technol. People, 2021.

[12] K. M. Hosny, A. M. Mortda, M. M. Fouda, and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," IEEE Access, vol. 10, pp. 48622–48632, 2022.

[13] K.-T. Huynh, T.-N. Ly, and T. Le-Tien, "An efficient model for copy-move image forgery detection," Int. J. Web Inf. Syst., no. ahead-of-print, 2022.

[14] W. Lu, W. Xu, and Z. Sheng, "An Interpretable Image Tampering Detection Approach based on Cooperative Game," IEEE Trans. Circuits Syst. Video Technol., 2022.

[15] E. U. H. Qazi, T. Zia, and A. Almorjan, "Deep Learning-Based Digital Image Forgery Detection System," Appl. Sci., vol. 12, no. 6, p. 2851, 2022.

[16] D. Mallick, M. Shaikh, A. Gulhane, and T. Maktum, "Copy Move and Splicing Image Forgery Detection using CNN," in ITM Web of Conferences, 2022, vol. 44, p. 3052.

[17] Kumar, K. U. Singh, C. Swarup, T. Singh, L. Raja, and A. Kumar, "Detection of Copy-Move Forgery Using Euclidean Distance and Texture Features.," Trait. du Signal, vol. 39, no. 3, 2022.

[18] E. Amiri, A. Mosallanejad, and A. Sheikhahmadi, "Copy-Move Forgery Detection by an

Optimal Keypoint on SIFT (OKSIFT) Method.," J. Comput. Robot., vol. 14, no. 2, pp. 11–19, 2021.

[19] Jain and N. Goel, "Advancements in Image Splicing and Copy-move Forgery Detection Techniques: A Survey," in 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2021, pp. 470–475.

[20] Chougala, G. Patil, and S. Kumar, "A REVIEW ON COPY MOVE FORGERY DETECTION IN DOCUMENT IMAGES."

[21] P. Yadav, "An Efficient and Effective Approach of Copy--Move Image Forgery Detection for Small Predefined Block Size," in Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems, 2022, pp. 955–963.

[22] S. Roy and K. Roy, "Block-Based Copy--Move Forgery Detection for Digital Image Forensic," in Proceedings of International Conference on Advanced Computing Applications, 2022, pp. 507–517.

[23] V. Kour, P. Aggarwal, and R. Kaur, "A Fast Block-Based Technique to Detect Copy-Move Forgery in Digital Images," in Recent Advances in Artificial Intelligence and Data Engineering, Springer, 2022, pp. 299–307.

[24] B. Gurunlu and S. Ozturk, "Efficient Approach for Block-Based Copy-Move Forgery Detection," in Smart Trends in Computing and Communications, Springer, 2022, pp. 167–174.

[25] N. Venu and B. K. Sujatha, "Enhanced block based copy paste image forgery detection," Mater. Today Proc., 2021.

[26] B. Soni and P. K. Das, "Geometric Transformation Invariant Improved Block-Based Copy-Move Forgery Detection," in Image Copy-Move Forgery Detection, Springer, 2022, pp. 51–67.

[27] Shahbahrami and F. Hoveyda, "Performance evaluation of block-based copy-move image forgery detection algorithms," Soft Comput. J., vol. 7, no. 1, pp. 62–79, 2021.

[28] M. Mokhtari Ardakan, M. Yerokh, and M. Akhavan Saffar, "A new method to copy-move forgery detection in digital images using Gabor filter," in Fundamental Research in Electrical Engineering, Springer, 2019, pp. 115–134.

[29] T. Jiang, Z. Cui, Z. Zhou, and Z. Cao, "Data augmentation with Gabor filter in deep convolutional neural networks for SAR target recognition," in IGARSS 2018-2018 IEEE International Geoscience and Remote Sensing Symposium, 2018, pp. 689–692.

[30] R. Singh, A. Goel, and D. K. Raghuvanshi, "Computer-aided diagnostic network for brain tumor classification employing modulated Gabor filter banks," Vis. Comput., vol. 37, no. 8, pp. 2157–2171, 2021.

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

[32] J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," 2003.

[33] H. A. Alberry, A. A. Hegazy, and G. I. Salama, "A fast SIFT based method for copy move forgery detection," Futur. Comput. Informatics J., vol. 3, no. 2, pp. 159–165, 2018.

[34] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in 2010 International Conference on Multimedia Information

Networking and Security, 2010, pp. 889–892.

[35] H.-Y. Huang and A.-J. Ciou, “Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation,” EURASIP J. Image Video Process., vol. 2019, no. 1, pp. 1–16, 2019.

[36] B. Xu, G. Liu, and Y. Dai, “A fast image copy-move forgery detection method using phase correlation,” in 2012 Fourth International Conference on Multimedia Information Networking and Security, 2012, pp. 319–322.

[37] N. D. Wandji, S. Xingming, and M. F. Kue, “Detection of copy-move forgery in digital images based on DCT,” arXiv Prepr. arXiv1308.5661, 2013.

[38] Saeed N. T., H. M. Ahmed, “Building a Real-Time System to Monitor Students Electronically Based on Digital Images of Face Movement,” pp. 83–88, 2022.