Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.1, February 2025, pp. 168~172
e-ISSN: 2548-6861

Analysis of Copy-move Manipulation in Digital Images using Scale Invariant Feature Transform (SIFT) and SVD-matching Methods

Muhamad Masjun Efendi [1]*, Nukman [2]**
* Sistem Informasi, Universitas Teknologi Mataram
** Teknologi Informasi, Institut Teknologi dan Kesehatan Aspirasi
creativepio@gmail.com [1], nukman.itka@gmail.comd [2]

Article Info

Article history:

Received 2024-11-21
Revised 2024-12-05
Accepted 2025-01-17

Keyword:

Manipulation,
Image,
Copy-move,
SIFT,
SVD-matching.

ABSTRACT

In recent years, more and more data has been created in digital form, allowing for easier control over storage and manipulation thanks to technological advancements. Unfortunately, these advancements also bring with them many risks, especially those related to the security of digital files. One of the concerns of many organisations is digital forgery, as it is increasingly easy to create fake images without leaving obvious traces of manipulation. One form of image forgery known as 'copy-move' is considered one of the most difficult problems in forgery detection. In this case, a portion of an image is copied and pasted at another location in the same image to hide unwanted objects in the scene. In this paper, we propose a method that automatically detects duplication areas within the same image. Duplication detection is performed by identifying local characteristics of the image (key points) using the Scale Invariant Feature Transform (SIFT) method and matching identical features using the Singular Value Decomposition (SVD) method. The results obtained show that our proposed hybrid method is robust to geometric transformations and is able to detect duplication areas with high performance.

I. INTRODUCTION

Digital image falsification is a concern for many people, with the help of image processing software the manipulation process becomes faster and easier to do, giving rise to a person's desire to manipulate images and usually before the image is published to the internet or other social media, the manipulation process is carried out first [1]. Although this activity is a common thing to do, it sometimes harms others and at the same time it is also a deception of the public about the truth of the image. In practice, image manipulation is often misused for certain interests [2]. So this is a big problem for many people, organisations, government or private [3]. Hoax content that circulates covers a variety of issues, some of which include negative content, especially using manipulated photos where the photos contain hate speech based on SARA (ethnicity, religion, race and intergroup) and hoaxes are rampant in the digital space. The Ministry of Communication and Informatics (Kominfo) noted that there were at least 12,547 hoax contents circulating between August 2018 and December 2023 [4]. As an action, Kominfo terminated access to the distribution of related content [5]. In the field of law, sometimes an image or picture is used as evidence in court. If an image submitted to the court is found to have been manipulated, even if it only adds a dot to the image, the integrity and validity of the image is lost and it can no longer be used as evidence in court [6]. Image falsification is the process of manipulating some or all regions of an image both in terms of content and context with the help of digital image processing techniques [7]. This requires high attention on how to detect the original image and the manipulated image. There are several types of image falsification, including cloning, rotating, scaling, retouching, copy-move, splicing etc [8]. One of the most common and frequently performed types of image forgery is Copy-move forgery because the technique is easily performed by many people. This forgery technique is based on copying a part of an image and then pasting the copied part onto another part of the image [9]. The following is an example of a Copy-move type manipulation image:

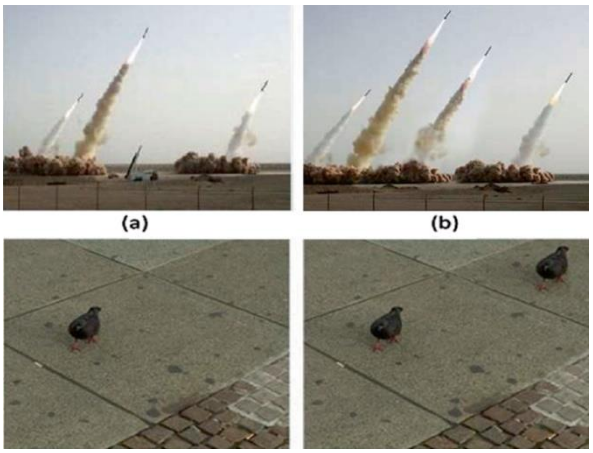

Figure 1. Image Illustration

Copy-move is the process of copying one part of an image and inserting it into another part of the same image at a different position [10]. With the existence of image forgery, it is important to authenticate digital images, identify the authenticity of a digital image and how to detect digital image forgery.

Due to the importance of knowing whether an image has been manipulated or not, an approach or technique that can analyse the changes that have occurred in the image is required. There are many methods used to solve the Copy-move type manipulation problem, but the detection accuracy of these methods is still lacking. Therefore, this research applies one of the methods to solve the above problem by using the Scale Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD)-matching methods. Image duplication detection is carried out by identifying the characteristics of the area of the image or image (points of interest) using the Scale Invariant Feature Transform (SIFT) method and by matching between identical features using the Singular Value Decomposition (SVD)-matching method.

Several other studies have discussed methods for solving Copy-move type manipulation. In the research conducted by [11] to perform image manipulation detection using the Discrete Cosine Transform (DCT) method, First, the image is separated into several overlapping blocks; after that, DCT sorting is performed in each local area or region of each block to identify similar blocks. Paper [12] presented an approach based on principal component analysis (PCA). PCA aims to reduce computational complexity by truncating vectors that have low significance. This technique is effective in overcoming small duplications in images, such as additive noise or lossy compression. Furthermore, paper [13] applies the blur moment invariant method, used to identify duplicated regions. The next paper written by [14] applies the wavelet transform method to the image to produce lower dimensions. After that, identifying similar blocks by using the log polar coordinates of the correlation stage as a criterion for similarity or similarity of image objects. The next paper written [15] proposes to extract image characteristics from image blocks by applying Fourier Mellin Transform (FMT). The next paper written by [16] applies the Singular Values Decomposition (SVD) method to extract feature vectors from each image block. Then, K-d trees are used to identify similar blocks. While the research conducted or written by [17] applies a technique based on Speed Up Robust features (SURF) [18] this method can detect object copy transfer forgery quickly and can withstand changes and processing such as scaling, rotation, and noise [19].

II. MATERIAL AND METHOD

The data collection process in this study uses the documentation method. Sample data is taken from photos obtained from the internet and from the results of personal cameras, namely, canon 5d mark II cameras, as well as from Xiaomi 13T mobile phones. Images or images that are used as data samples are selected image models with different backgrounds. Then the image is processed using Adobe Photoshop 2024 image processing software to perform a Copy-move process where the size of the Copy-move area varies, while the other images are left in their original condition. The software requirements needed as described above are image editing software, Matlab for writing source code and software for creating system designs.

We propose a method to identify the location of duplicated regions within the same image. This method aims to detect copy-paste forgeries by analyzing local image descriptors using the SIFT technique and matching identical descriptors through Singular Value Decomposition (SVD) [20] [21]. The various steps involved are clearly illustrated in Figure 2.

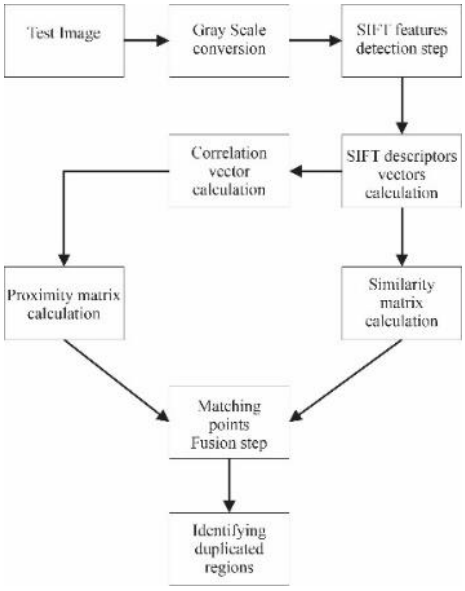

Figure 2. Flow chart Workflow System

There are 3 main steps in this method:

A. SIFT descriptors extraction

In the first step, we applied the SIFT transform to the input image to extract key-points, which are described by 128-

dimensional descriptor vectors and their positions (row, column, scale, orientation). These key-points are considered invariant descriptors, as they are unaffected by rotation, scaling, and translation, and are also robust to changes in illumination, noise, and slight variations in viewpoint. The SIFT algorithm consists of four stages: scale-space peak detection, key-point localization refinement, orientation assignment, and key-point descriptor generation.

Here's a summary of each stage: The first stage identifies interest points in the image that are invariant to scale and orientation by detecting maxima and minima from a series of Difference of Gaussian images created at multiple scales across the image. In the second stage, additional features are extracted from the detected key-points, and fewer stable points are eliminated by calculating the Laplacian value for each key-point. The third stage assigns dominant orientations to each key-point based on its local image patch, allowing SIFT to generate a canonical view for each key-point that is invariant to similarity transforms. Finally, in the fourth stage, a local feature descriptor is computed for each key-point based on the surrounding pixel patch. The result of this process is a set of SIFT key-points represented by 128-dimensional descriptor vectors and their positions (row, column, scale, and orientation).

B. Descriptors matching strategy

The second step of the method involves matching the extracted descriptors. To accomplish this, we calculate the similarity matrix and the proximity matrix from the SVD factorization, then combine the results from these two matrices [22].

C. Duplicated regions detection

The final step aims to display the image with the correctly matched points, using the location (row and column), scale, and orientation of each pair of SIFT features to highlight the copied and pasted regions.

III. Results And Discussion

The proposed approach was fully implemented in MATLAB and tested on 30 images with diverse content. These images were free from any other forms of tampering. Some of the images were manipulated using geometric modifications, such as rotation and scaling. The following section presents and discusses the results of the forgery detection.

All results were obtained with a correlation threshold set as low as 0.6. Table 1 presents the number of false matches (determined through visual inspection) for the image pairs tested below, in relation to variations in σ, expressed as a fraction of the image width. The table indicates that the selection of the parameter σ in equation (2) across a relatively wide range has minimal impact on performance. Consequently, σ is set to 1/6 of the image width for all test images.

TABLE 1.
SENSITIVITY OF RESULTS TO VARIATIONS OF Σ

σ/(image _width)	Numbers of mismatches			
	Image 1	Image 2	Image 3	Image 4
1/2	2	4	3	4
1/4	2	4	4	4
1/6	1	3	3	2
1/8	3	4	4	3

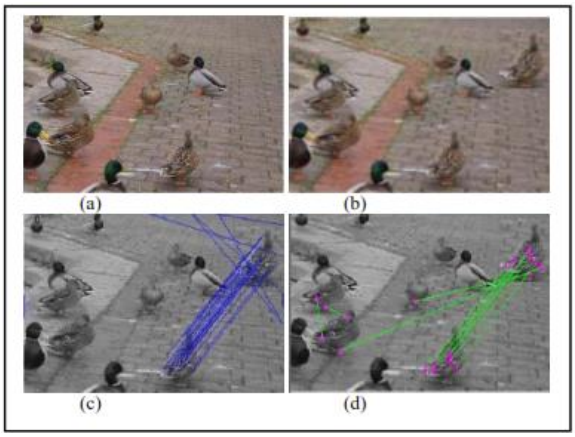

Figure 3. (a) Original test image, (b) doctored image where the copied region has undergone no further distortion and (c), (d) the obtained results.

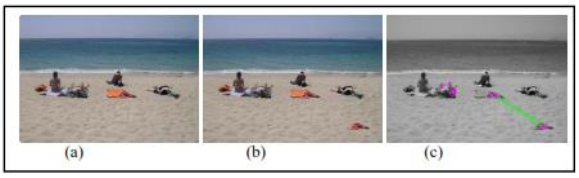

Figure 4. (a) Original test image, (b) doctored image where the copied region has undergone no further distortion and (c) the obtained results.

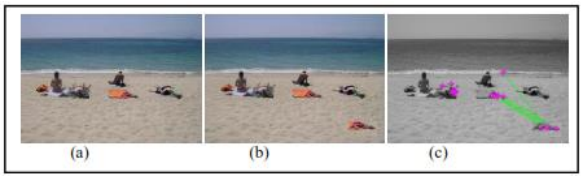

Figure 5. (a) Original test image, (b) doctored image where the copied region has undergone 65% scaling and (c) the obtained result.

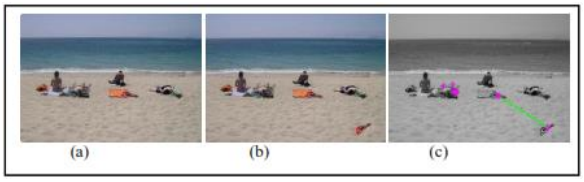

Figure 6. (a) Original test image, (b) doctored image where the copied region has undergone 50° rotation and (c) the obtained result.

Some previous results show false detections indicated by one or two green lines. However, these lines do not represent forgery, as they do not appear in clusters. Duplicated regions

are considered detected when the result shows a cluster of green lines, marking the copy-paste areas.

The experimental results with false matching indicate that this approach may become impractical for images with a large number of features, as seen in Figures 4, 5, and 6 (with over 3000 features). Additionally, the number of false matches in Figure 3 demonstrates that our method, based on SIFT descriptors, is not effective at detecting forgeries in smooth regions like deserts, skies, and similar areas.

IV. CONCLUSION

In this paper, we propose a method to detect duplicated image areas using Scale Invariant Feature Transform (SIFT) and SVD-matching methods. The SIFT algorithm first detects key points in the image, which are unique local features, such as corners, edges, or conspicuous points. After detecting the key points, SIFT creates a descriptor for each key point. This descriptor is a vector that represents the intensity pattern of the pixels around the key point. These descriptors are resistant to changes in scale, rotation, and translation, so the features of the same image will remain consistent even if the image undergoes geometric changes. The descriptors of the original image and the suspected manipulated image are compared to find matches between the key points. If there are many matching key points in two different regions of the image, it indicates duplicated areas. SVD-matching, on the other hand, involves dividing the image into small blocks. Then, each block is decomposed using SVD, so that the block is represented by singular values that represent the important characteristics of the block. The singular values of each block are compared with other blocks in the image. If there are blocks with very similar singular values, this could indicate that the blocks are duplicated or manipulated. Testing using 30 images, this image dataset is taken from the canon 5d mark II camera and Xiaomi 13T mobile phone. Each 15 original images, and 15 edited images. These 15 original images are left as they are without making changes, editing or manipulation, while the other 15 images are changed, edited or manipulated using editing software. The results of editing manipulation with the copy-move technique successfully detected the manipulated image objects accurately and well.

Scale Invariant Feature Transform (SIFT) method is very effective in detecting duplication even if the image undergoes transformations such as rotation, scaling, or translation. Meanwhile, SVD enables data dimensionality reduction, making feature matching more efficient and faster.

While robust to geometric transformations, SIFT can be less effective if there are large changes in texture or lighting. And while SVD can match blocks effectively, it gives an incorrect matching rate if the image has many naturally similar blocks. In general, the results showed promising results. In future research, we plan to further refine this method to reduce the false matching rate.

ACKNOWLEDGEMENTS

We gratefully acknowledge the generous support provided by all parties both from family and colleagues so that this research can be completed.

REFERENCES

[1] I. T. Ahmed, B. T. Hammad, and N. Jamil, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," *Proceeding - 2021 IEEE 17th Int. Colloq. Signal Process. Its Appl. CSPA 2021*, no. March, pp. 92–96, 2021, doi: 10.1109/CSPA52141.2021.9377272.

[2] A. Aimen, A. Kaur, and S. Sidheekh, "Scale Invariant Fast PHT based Copy-Move Forgery Detection," *2020 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020*, 2020, doi: 10.1109/ICCCNT49239.2020.9225276.

[3] M. Salman and A. Uhl, "Countering anti-forensics of SIFT-based copy-move detection," *Proc. - Int. Conf. Pattern Recognit.*, pp. 2701–2707, 2020, doi: 10.1109/ICPR48806.2021.9413012.

[4] B. G. Rosy Dewi Arianti Saptoyo, "Kominfo Temukan 12.547 Konten Hoaks 5 Tahun Terakhir." kompas, Jakarta, 2024. [Online]. Available: https://www.kompas.com/

[5] Hanifah Triari Husna, "Sampai Mei 2023, Kominfo Identifikasi 11.642 Konten Hoaks." kominfo, Jakarta, 2023. [Online]. Available: https://aptika.kominfo.go.id/

[6] R. S. Khalaf and A. Varol, "Digital forensics: Focusing on image forensics," *7th Int. Symp. Digit. Forensics Secur. ISDFS 2019*, pp. 1–5, 2019, doi: 10.1109/ISDFS.2019.8757557.

[7] R. Ashraf, M. S. Mehmood, T. Mahmood, J. Rashid, M. W. Nisar, and M. Shah, "An Efficient Forensic Approach for Copy-move Forgery Detection via Discrete Wavelet Transform," *1st Annu. Int. Conf. Cyber Warf. Secur. ICCWS 2020 - Proc.*, 2020, doi: 10.1109/ICCWS48432.2020.9292372.

[8] X. Bi, Z. Zhang, Y. Liu, B. Xiao, and W. Li, "Multi-Task Wavelet Corrected Network for Image Splicing Forgery Detection and Localization," *Proc. - IEEE Int. Conf. Multimed. Expo*, 2021, doi: 10.1109/ICME51207.2021.9428466.

[9] T. Nazir, A. Irtaza, A. Javed, H. Malik, A. Mehmood, and M. Nawaz, "Digital Image Forensic Analysis using Hybrid Features," *2021 Int. Conf. Artif. Intell. ICAI 2021*, pp. 33–36, 2021, doi: 10.1109/ICAI52203.2021.9445228.

[10] K. Sunitha and A. N. Krishna, "Efficient Keypoint based Copy Move Forgery Detection Method using Hybrid Feature Extraction," *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 670–675, 2020, doi: 10.1109/ICIMIA48430.2020.9074951.

[11] M. S. Rana, M. M. Hasan, and S. K. S. Shuva, "Digital Watermarking Image Using Discrete Wavelet Transform and Discrete Cosine Transform with Noise Identification," *2022 2nd Int. Conf. Intell. Technol. CONIT 2022*, no. August, pp. 1–5, 2022, doi: 10.1109/CONIT55038.2022.9847745.

[12] W. Y. Min, E. Romanova, Y. Lisovec, and A. M. San, "Application of statistical data processing for solving the problem of face recognition by using principal components analysis method," *Proc. 2019 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2019*, no. 1, pp. 2208–2212, 2019, doi: 10.1109/EIConRus.2019.8657240.

[13] J. Flusser, S. Farokhi, C. Höschl, T. Suk, B. Zitová, and M. Pedone, "Recognition of images degraded by Gaussian blur," *IEEE Trans. Image Process.*, vol. 25, no. 2, pp. 790–806, 2016, doi: 10.1109/TIP.2015.2512108.

[14] B. Fan *et al.*, "A performance evaluation of local features for image-based 3D reconstruction," *IEEE Trans. Image Process.*, vol. 28, no. 10, pp. 4774–4789, 2019, doi: 10.1109/TIP.2019.2909640.

[15] J. Thayyil and K. Edet Bijoy, "Digital Image Forgery Detection using Graph Fourier Transform," *Int. Conf. Futur. Technol. Control Syst. Renew. Energy, ICFCR 2020*, pp. 1–5, 2020, doi: 10.1109/ICFCR50903.2020.9249969.

[16] A. Kaur, S. Walia, and K. Kumar, "Comparative Analysis of Different Keypoint Based Copy-Move Forgery Detection Methods," *2018 11th Int. Conf. Contemp. Comput. IC3 2018*, pp. 1–5, 2018, doi: 10.1109/IC3.2018.8530489.

[17] K. Ramirez-Gutierrez, Mariko-Nakano, G. Sanchez-Perez, and H. Perez-Meana, "Copy-move forgery detection algorithm using frequency transforms, surf and mser," *2019 7th Int. Work. Biometrics Forensics, IWBF 2019*, pp. 1–6, 2019, doi: 10.1109/IWBF.2019.8739168.

[18] J. He, Y. Xie, X. Luan, X. Niu, and X. Zhang, "A TV logo detection and recognition method based on SURF feature and bag-of-words model," *2016 2nd IEEE Int. Conf. Comput. Commun. ICCC 2016 - Proc.*, pp. 370–374, 2017, doi: 10.1109/CompComm.2016.7924725.

[19] D. Mahalakshmi and C. Science, "Copy - Move Image Forgery Detection System Using Hybrid Method," *Int. J. Eng. Sci. Invent. Res. Dev.*, vol. III, no. XI, pp. 692–698, 2017.

[20] W. Song, X. Hu, J. Fu, Q. Zhou, T. Zhou, and P. Si, "The method of hybrid-laser image spot extracts based on HSV space SVD for power transmission line detection," *2016 IEEE Int. Conf. Inf. Autom. IEEE ICIA 2016*, no. August, pp. 1361–1364, 2017, doi: 10.1109/ICInfA.2016.7832031.

[21] S. Bhosale, G. Thube, P. Jangam, and R. Borse, "Employing SVD and wavelets for digital image forensics and tampering detection," *Proc. 2012 Int. Conf. Adv. Mob. Networks, Commun. Its Appl. MNCApps 2012*, pp. 135–138, 2012, doi: 10.1109/MNCApps.2012.35.

[22] A. Kashyap, M. Agarwal, and H. Gupta, "Detection of copy-move image forgery using SVD and cuckoo search algorithm," *Int. J. Eng. Technol.*, vol. 7, no. 2, pp. 79–87, 2018, doi: 10.14419/ijet.v7i2.13.11604.