Journal of Applied Informatics and Computing (JAIC)
Vol.8, No.2, December 2024, pp. 408~412
e-ISSN: 2548-6861

Analysis of Splicing Manipulation in Digital Images using Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) Methods

Zumratul Muhidin [1]*, Nasirudin Karim [2]*, Muhamad Masjun Efendi [3]*
* Sistem Informasi, Universitas Teknologi Mataram
** Rekayasa Siste Komputer, Universitas Teknologi Mataram
*** Sistem Informasi, Universitas Teknologi Mataram
muahidinzumratul@gmail.com [1], karimmuhnasirudin@gmail.com [2], creativepio@gmail.com [3]

Article Info

Article history:

Received 2024-09-21
Revised 2024-10-01
Accepted 2024-10-02

Keyword:

Manipulation,
Image Splicing,
DyWT,
SIFT.

ABSTRACT

In the digital age, image manipulation is common, often done before publication on social media. However, this can lead to negative impacts, including visual deception. This research aims to detect splicing type image manipulation using Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) methods. The process starts with image decomposition using DyWT to obtain LL sub-images, followed by local feature extraction using SIFT. An application built on desktop-based Matlab source was developed to detect splicing forgery in digital images. The test used 20 images, this image dataset was taken from canon 5d mark II camera and Vivo X80 mobile phone. Each 10 original images, and 10 edited images. These 10 original images are left as they are without making changes, editing or manipulation, while the other 10 images are changed, edited or manipulated using editing software, the results of this editing are uploaded to social media, such as Facebook and Instagram, which will later be used as datasets in testing. The results show that the splicing technique is detected accurately, and processing is faster on images with low pixel resolution. The DyWT and SIFT methods are effective in detecting post-processing attacks such as rotation and rescaling, although they have drawbacks. DyWT struggles in detecting subtle changes and noise, while SIFT is less effective on non-geometric manipulations. Overall, both methods face challenges in detecting complex manipulations and require significant computational resources, especially on high-resolution images.

I. PENDAHULUAN

Falsification of digital images in today's technological development is very common. This can cause problems in social life such as loss of trust in news, defamation, damage to one's reputation, falsification of evidence and many other problems. Image falsification is the process of manipulating some or all of the image regions both on the content and context of the image with the help of digital image processing techniques [1]. Although this activity is a common thing to do, it sometimes harms others and at the same time it is also a public deception about the truth of the image. In practice, image manipulation is often misused for certain purposes [2]. Negative content, especially using manipulated photos that contain hate speech based on SARA (ethnicity, religion, race and intergroup) and hoaxes, is rampant in the digital space.

Based on data from the Ministry of Communication and Informatics (Kemenkominfo), from 2019-2023, there were 4,640 contents in the digital space that were taken down by Kemenkominfo for causing hatred or hostility, which was caused by manipulated photos. Throughout 2023, Kemenkominfo also followed up on 1,517 hoax issues circulating on social media, many of which used photos to spread the hoax [3]. 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 [4].

There are several purposes in performing manipulation, such as humour, entertainment, sensation, economics, education or even more extreme is to spread hatred and slander [5]. There are several types of image falsification, including cloning, rotating, scaling, retouching, copy-move, splicing etc. One form of digital image manipulation that is often done is splicing manipulation. Splicing is duplicating a certain part of one or more images and placing it in a certain part of the target image or a different image [6]. The following is an example of a splicing type manipulation image.

Figure 1. Illustration of image splicing

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 problem of splicing manipulation, but the detection accuracy of these methods is still lacking. Therefore, in this research, one method is applied to solve the above problem by using the Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT) methods. The Dyadic Wavelet Transform (DyWT) method works by analysing and reconstructing data by utilising small waves (wavelets) as its basis function. DyWT works by dividing the signal or image into small parts called sub-blocks, then applying a wavelet transformation to each sub-block [7], while the Scale Invariant Feature Transform (SIFT) method has several stages in detecting image matches, namely Scale Space Extreme, Keypoin Localizaton, Orientation Assigment and Keypoint Descriptor [8]. By using this method, the expected results will be able to improve the accuracy of splicing manipulation detection properly and accurately.

Several other studies have discussed methods of solving splicing type manipulation. In the research conducted by [9] to detect splicing type image manipulation using the Gaussian blur method. Gaussian blur inconsistency is used to test the authenticity of the image. The Gaussian blur of the first image is evaluated and the obtained standard deviation is used to blur the image. The results can be used to detect forged regions that are highly blurred, but images with splicing in them are less accurately detected and this algorithm works well only with Gaussian blur type forgeries. In the paper written [10], a combination of five algorithms is used to detect splicing. In general, the proposed method resulted in an accuracy of more than 75%. Meanwhile, the research conducted by [11-17] highlights the inconsistency of local noise in quadtree image scanning. This method can detect splicing in raw digital images, but in small splicing areas it is unable to detect splicing properly and accurately.

II. METHODS

The methodology used in this research is as follows:

A. *Data Collection Methods*

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 Vivo X80 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 the splicing process where the size of the spliced area varies, while the other images are left in their original condition. The software used includes image editing software, Matlab for writing source code, and software for designing the system.

B. *System Design*

The following is a flowchart in detecting image authenticity using the DyWT and SIFT algorithms in the matlab code.

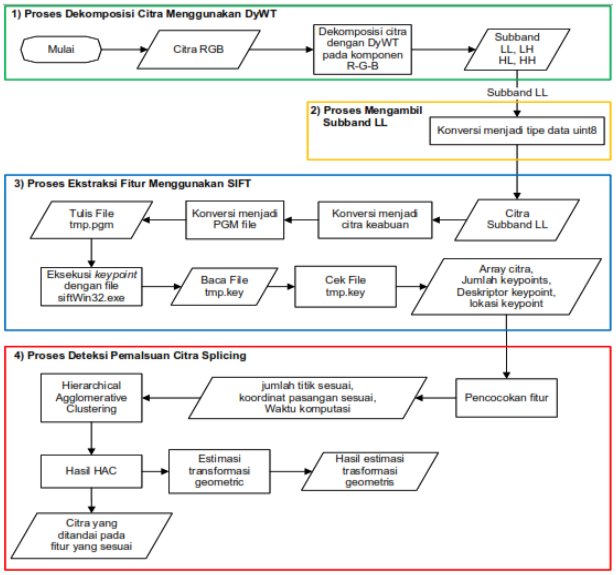

Figure 2. *Flow chart Workflow System*

Broadly speaking, the image splicing forgery detection process in this simulation consists of 4 stages, namely the image decomposition process using DyWT, the second process of taking LL subbands, the third image extraction process using SIFT, and the fourth image manipulation detection process of the splicing type.

III. RESULTS AND DISCUSSION

Tests are conducted on various images with different image sizes and dimensions. The test images were subjected to conditions or attacks with different sizes of the forgery area and different geometric image processing manipulations. System testing is carried out on the original image and the image with splicing type forgery. The following tests were carried out in this study.

A. Test Results Against Original Image

In testing the original image is done with the original image. The test image used is 10 original images.

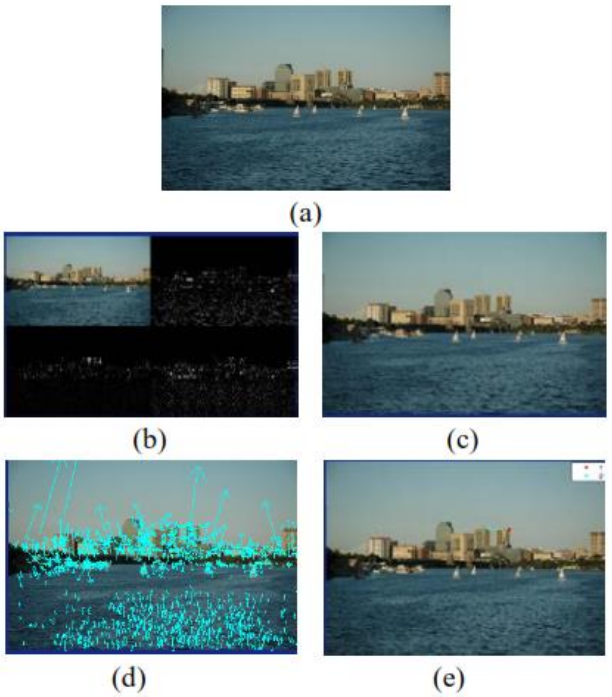

Figure 3. (a) input image. (b) result image DyWT. (c) image subband LL (d) feature extraction result SIFT. (e) image detection result. Figure 3 shows the various processes that occur in testing the application on images without splicing forgery. Figure 3(a) is the input image processed by the application. The input image is decomposed using the DyWT method, resulting in image 3(b). From the decomposition results, the LL subband is then taken as the image to be processed as in Figure 3 (c). The LL subband image is then feature extracted using the SIFT method, resulting in a display as shown in Figure 3 (d). After obtaining the features of the LL subband, the detection process is carried out to obtain the detection results as shown in Figure 3 (e).

TABLE 1.
TEST RESULTS AGAINST THE ORIGINAL IMAGE

No	Data	Keypoint	Detection time	Detection result
1	Image 1	6824	67.826	original
2	Image 2	517	0.87774	original
3	Image 3	2732	3.21083	original
4	Image 4	1753	8.17356	original
5	Image 5	475	0.21867	original
6	Image 6	5662	46.585	original
7	Image 7	1897	9.18264	original
8	Image 8	2092	1.83723	original
9	Image 9	1520	6.79425	original
10	Image 10	627	0.21867	original

B. Test Results of The Manipulated Image

In the second test, the manipulation process is carried out on the image to be tested. The test image data used is 10 images.

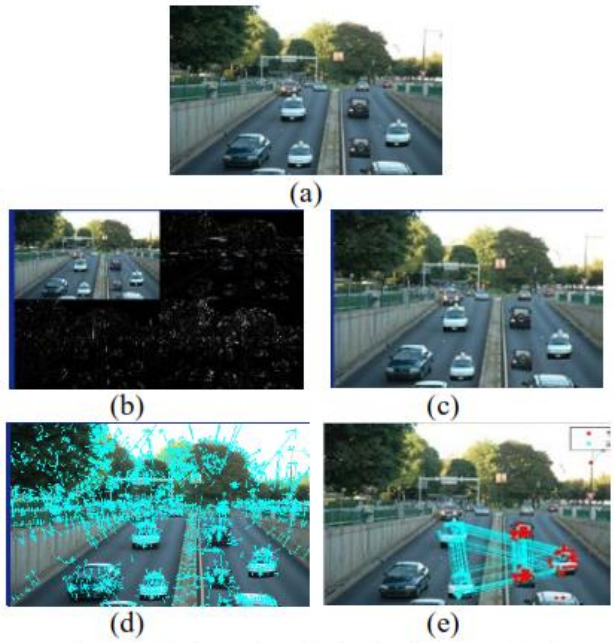

Figure 4. (a) false image. (b) result image DyWT. (c) image subband LL (d) feature extraction result SIFT. (e) image detection result. Figure 4 shows the processes involved in detecting image forgery in the system. The input image tested is the fake image shown in Figure 4 (a). The system successfully detects the splicing forgery shown in Figure 4 (e).

TABLE 2.
TEST RESULTS AGAINST FAKE IMAGES

No	Data	Attack	Keypoint	Detection time	Detection result
1	Image 1	Scale scaled down x = 0.9 y = 0.9	3834	7.64356	fake
2	Image 2	Rotation 10^o Scale Enlarged x = 1.4 y = 1.2	3871	7.79565	fake
3	Image 3	Scale Enlarged x = 2.0 y = 1.6	3864	7.82095	fake
4	Image 4	Scale scaled down x = 1.2	3877	7.66033	fake

		y = 1.2			
5	Image 5	Rotation 45º Scale Enlarged x = 1.2 y = 1.5	3845	7.69284	fake
6	Image 1	Skala diperkecil x = 1.4 y = 1.4	3846	7.47538	fake
7	Image 2	Rotation 35º Scale scaled down x = 0.7 y = 0.7	3846	7.62604	fake
8	Image 3	Scale scaled down x = 1.5 y = 1.5	3854	7.37862	fake
9	Image 4	Rotation 20º Scale Enlarged x = 2.4 y = 1.5	3892	7.81515	fake
10	Image 5	Scale Enlarged x = 1.3 y = 1.6	3888	7.81287	fake

IV. CONCLUSION

This research has produced an application made using desktop-based Matlab that is able to detect splicing forgery in digital images using the Dyadic Wavelet (DyWT) and Scale Invariant Feature Transform (SIFT) methods. Testing using 20 images, this image dataset is taken from the canon 5d mark II camera and Vivo X80 mobile phone. Each 10 original images, and 10 edited images. These 10 original images are left as they are without making changes, editing or manipulation, while the other 10 images are changed, edited or manipulated using editing software. The results of editing manipulation with the splicing technique successfully detected the manipulated image objects accurately and well. The time taken in image processing is faster in images that have lower pixel resolution compared to images that have higher pixel resolution. This is because each pixel needs to be analysed, calculated, and processed during image processing stages, such as filtering, transformation, or feature detection. The more pixels there are, the more calculations need to be performed, thus slowing down the processing. High-resolution images usually have larger file sizes, which means they require more memory and time to be read, written or moved during processing. This can also extend the time in steps such as image compression or decompression. Based on the test results, it is known that the application of Dyadic Wavelet (DyWT) and Scale Invariant Feature Transform (SIFT) methods is able to detect post-processing attacks with rotation and scale falsification (enlarged and reduced) methods applied to the test image. Discrete Wavelet Transform (DyWT), DyWT breaks the image into different frequency components, thus capturing both high and low frequency information from the image. This method tends to be more resilient to changes in scale as the analysis is performed at various resolution levels that capture the texture details of the original image. When the image is rotated or rescaled, the underlying frequency components remain consistent, so DyWT is able to detect any discrepancies due to manipulation despite basic transformation changes such as rotation or rescaling. As for the Scale Invariant Feature Transform (SIFT) method, SIFT is designed to be scale and rotation invariant. The SIFT algorithm detects 'keypoints' in the image that are not affected by rotation or resizing. This detection process is done by computing local descriptors that include directional and scale information. The resulting features remain consistent even if the image is rotated or rescaled, making SIFT very effective in detecting manipulations on images that have undergone such geometric modifications. Therefore, even if the image has undergone manipulations such as rotation or rescaling, DyWT and SIFT are still effective as they both utilise the underlying information of the image that is independent of changes in orientation or size. Although DyWT (Discrete Wavelet Transform) and SIFT (Scale-Invariant Feature Transform) methods are effective in detecting digital image manipulation, they have some disadvantages. DyWT tends to struggle in detecting subtle changes in image details and is susceptible to noise interference, as well as being less than optimal for detecting localised or small-area manipulations. Meanwhile, SIFT is susceptible to non-geometric manipulations such as colour or lighting changes, and is not effective in handling subtle changes in non-dominant features. Both also face difficulties in detecting complex manipulations involving a combination of techniques, and SIFT is computationally intensive, making it less ideal for high-resolution images or real-time processing. In general, carefully performed subtle manipulations or extreme changes in image conditions can weaken the ability of these two methods to effectively detect forgery. For future research a hybrid approach by combining DyWT and SIFT with other detection methods, such as deep learning-based algorithms or neural networks models, can help detect non-geometric manipulations such as colour or texture changes, to overcome lighting manipulations and subtle changes in the image, additional algorithms focusing on global features and spectral analysis can be applied to provide a broader context, so that local and global manipulation detection can be more accurate.

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] J. Charpe and A. Bhattacharya, "Revealing image forgery through image manipulation detection," *Glob. Conf. Commun. Technol. GCCT 2015*, no. Gcct, pp. 723–727, 2015, doi: 10.1109/GCCT.2015.7342759.

[2] I. T. Ahmed, B. T. Hammad, and N. Jamil, "A comparative analysis of image copy-move forgery detection algorithms based on hand and machine-crafted features," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 22, no. 2, pp. 1177–1190, 2021, doi: 10.11591/IJEECS.V22.I2.PP1177-1190.

[3] M. H. Andrian Saputra, "Fenomena Ujaran Kebencian Di Medsos," *Republika*. republika.co.id, Jakarta, pp. 1–3, 2022. [Online]. Available: https://islamdigest.republika.co.id/berita/rinxua430/fenomena-ujaran-kebencian-di-medsos

[4] S. S. Narayanan and G. Gopakumar, "Recursive Block Based Keypoint Matching for Copy Move Image Forgery Detection," *2020 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020*, 2020, doi: 10.1109/ICCCNT49239.2020.9225658.

[5] M. T. Jijina, L. Koshy, and G. S. Warrier, "Detection of Recoloring and Copy-Move Forgery in Digital Images," *Proc. - 2020 5th Int. Conf. Res. Comput. Intell. Commun. Networks, ICRCICN 2020*, pp. 49–53, 2020, doi: 10.1109/ICRCICN50933.2020.9296173.

[6] G. Bobashev, N. G. Baldasaro, K. C. Mills, and J. L. Davis, "An Efficiency-Decay Model for Lumen Maintenance," *IEEE Trans. Device Mater. Reliab.*, vol. 16, no. 3, pp. 277–281, 2016, doi: 10.1109/TDMR.2016.2584926.

[7] 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.

[8] T. Das, R. Hasan, M. R. Azam, and J. Uddin, "A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform," *Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2018*, pp. 1–4, 2018, doi: 10.1109/IC4ME2.2018.8465668.

[9] P. Dingbang, C. Hao, S. Xiaochong, and L. Jianxun, "Motion blurred star image centroid optimized extraction based on prior Gaussian distribution," *Proc. 29th Chinese Control Decis. Conf. CCDC 2017*, pp. 3149–3154, 2017, doi: 10.1109/CCDC.2017.7979049.

[10] Y. Fan and Helbert, "Detection of Image Splicing using Illuminant Color Estimation," 2019.

[11] T. Julliand *et al.*, "Automated Image Splicing Detection from Noise Estimation in Raw Images To cite this version : HAL Id : hal-01510075 Automated Image Splicing Detection from Noise Estimation in Raw Images," 2017.

[12] T. Julliand, V. Nozick, and H. Talbot, "Automated image splicing detection from noise estimation in raw images," *IET Semin. Dig.*, vol. 2015, no. 5, 2015, doi: 10.1049/ic.2015.0111.

[13] D. E. Kurniawan and N. Narupi, "Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijndael dan Steganografi Least Significant Bit (LSB)", JuTISI, vol. 2, no. 3, Dec. 2016.

[14] D. E. Kurniawan, N. R. Hartadi, and P. Prasetyawan, "Analisis Hasil Teknik Penyembunyian Hak Cipta Menggunakan Transformasi DCT dan RSPPMC pada Jejaring Sosial," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 5, no. 3, Art. no. 3, Aug. 2018, doi: 10.25126/jtiik.201853692.

[15] K. H. Hingrajiya and R. K. Sheth, "Comparative Study of Digital Image Forgery Detection Techniques," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 83-86, doi: 10.1109/ICACITE51222.2021.9404748.

[16] E. A. Armas Vega, E. González Fernández, A. L. Sandoval Orozco and L. J. García Villalba, "Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression," in IEEE Access, vol. 8, pp. 11815-11823, 2020, doi: 10.1109/ACCESS.2020.2964516.

[17] H. Tomita and T. Minamoto, "Detection of Stained Chrysotile in Microscopic Images Using Wavelet-Based Texture Features," 2022 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR), Toyama, Japan, 2022, pp. 19-24, doi: 10.1109/ICWAPR56446.2022.9947130.