ILKOM Scientific Journal Vol. 16, No. 3, December 2024, pp. 321-381
Accredited 2nd by RISTEKBRIN No. 200/M/KPT/2020; E-ISSN 2548-7779 | P-ISSN 2087-1716

A Comparative Analysis of Forensic Similarity and Scale Invariant Feature Transform (SIFT) for Forensic Image Identification

Muhammad Na'im Al Jum'ah [a,1,*]; Hamid Wijaya [a,2]; Suwito Pomalingo [b,3]
[a] *Universitas Sembilanbelas November Kolaka, Jl. Pemuda, Kolaka and 93514, Indonesia*
[b] *Multimedia Nusantara University, Jl. Scientia Boulevard, Tangerang and 15810, Indonesia*
[1] *muhnaimaljumah@usn.ac.id;* [2] *hamidwijaya@usn.ac.id;* [3] *suwito.pomalingo@umn.ac.id*
** Corresponding author*

Article history: Received September 13, 2024; Revised December 03, 2024; Accepted December 29, 2024; Available online December 31, 2024

Abstract

The image manipulation process has contributed to the widespread dissemination of false information. image forensics can help law enforcement agencies in addressing the spread of false news or information issues through visual media. Forensic image identification can be conducted using various methods, including Scale Invariant Feature Transform (SIFT) and Forensic Similarity. This study compared two methods, SIFT and Forensic Similarity, for forensic image identification. The test results showed the SIFT method identified image forensics by detecting image similarity through calculation of the key point values of each image. The process of searching the key point values was performed to extract information from the image. A high key point value indicated a large amount of information obtained from the image extraction results. On the other hand, the Forensic Similarity method also performed image forensic detection by examining whether image patches shared the same forensic traces. The advantage of the Forensic Similarity method over the SIFT method was that Forensic Similarity was more detailed because it involved many processes. Thus, Forensic Similarity was able to find similarities between two image patch objects. Additionally, the results obtained from the Forensic Similarity method were more detailed in detecting image similarity by considering the key point matching value and Cosine Similarity. Several previous studies have already implemented the SIFT and Forensic Similarity methods for image forensics, but there was no research that directly compared these two methods. This is the strength of this research. However, this study only used three data samples from three different devices for data collection. Future research can use a larger sample size to observe the comparison results.

Keywords: Digital Forensics; Forensic Similarity; Image Forensic; Scale Invariant Feature Transform (SIFT).

Introduction

The rapid advancement of technology makes the process of manipulation images much easier [1]. This ease can result in the creation and dissemination of false images and disinformation online [2]. Digital images have become an important information medium for many people. The available tools for digital image manipulation allow people to commit crimes [3]. In addition, the results of digital image manipulation are difficult to identify either they use real or fake images [4]. The dissemination of fake images is used to spread racial hatred, false narratives, or defamation about certain ethnic groups and political figures [5]. Image forgery is done by using digital imagery to change its semantic description [6]. One method to do counterfeiting detection is by using watermarking to extract embedded information from the input image [7]. Advancements in artificial intelligence technology have led to the creation of falsified photos that are more difficult to distinguish from the original ones [8].

Identification of digital images presents a significant challenge in the field of image forensics [9]. One method for identifying the source of the digital image can be performed by identifying the device used to capture the image [10]. This process is called image forensics. It will find the metadata of a digital image content. The metadata will provide information from a file [11]. Moving image segments from one location to another within the same image, called copy-move, allows the image to undergo changes in various characteristics such as noise, color, contrast, or other features of the original image [12]. The digital image verification process will determine whether the disseminated images have the same or different forensic traces [13]. The Forensic Similarity approach based on the Convolutional

Neural Network can be performed by comparing two different images from two different image capture scenarios [14]. The advantage of this approach is that it can compare models that are not used during the system's training phase [15].

The process of detecting the match between two different images can also be done with the Scale Invariant Feature Transform method [16]. This method has a higher accuracy in image matching compared to other methods [17]. Addressing this issue above requires the application of digital forensic action. Digital forensics is an important instrument in identifying and solving computer-based crimes and computer-aided crimes [18]. Some ways to verify digital images are to check the similarity of the compared images [19]. This verification process can be carried out by utilizing the Forensic Similarity method [15] and the Scale Invariant Feature Transform (SIFT) method [20].

The process of detecting the original source of digital images can serve as crucial supporting evidence to solve the case of spreading false information, a challenge faced by investigators [21]. However, the process of validating digital evidence requires a systematic method to prove the validity of the digital evidence [22]. A method is needed to check or validate images that have been disseminated, the process of checking or validating images can be performed by the Forensic Similarity and SIFT methods. Therefore, a comparison of Forensic Similarity and SIFT methods was carried out in the current study for forensic image identification. The purpose of this study was to introduce a new approach for verification of digital by employing these two methods concurrently. The combination of these two methods would identify the authenticity of the image by checking the source, metadata and object compatibility of the digital image.

Method

To address the above issue, the author implemented several strategies to support the solution presented in this study, including:

A. Literature Studies

The current research conducted reviews on related references and literature to problems and methods used to solve the addressed issue. This research was highly dependent on the existence of secondary data and the successful acquisition of primary data. Secondary data that supported this research were previous studies that contained methods and objects evaluating the methods. The primary data in this study was a similar object that can test the developed method.

B. Method Comparison

The purpose of this study was to compare the Forensic Similarity and SIFT methods for image identification carried out by digital forensics. The comparison of these two methods aimed to find out the advantages and disadvantages of conducting digital forensic image analysis of the two methods.

- Forensic Similarity Method

Forensic Similarity is a method to determine whether two image patches have the same or different forensic traces. Forensic Similarity based on the Convolutional Neural Network would also identify if two image patches were taken from the same or different camera models [23] [24]. However, this forensic approach differed from others in the way that it did not explicitly identify a particular forensic trace in an image patch, but it analyzed whether the forensic trace was consistent with the two image patches [25]. The main advantage of this method was that prior forensic information was not required to make a decision on the similarity of the forensic traces of the tested two image patches [15].

The forensic similarity system consisted of two elements, namely CNN-based feature extraction which mapped the input images to a low-dimensional feature space that encoded high-level forensic information, This phase was called the learning phase by training feature extraction [26] and the second was a three-layer neural network, commonly called a similarity network by mapping pairs of features into a score whether two image patches contained the same forensic footprint. This phase would train the network of similarities [27].

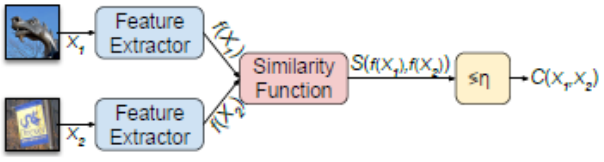


Figure 1. Forensic Similarity System

- Scale Invariant Feature Transform *(SIFT)* Method

Scale Invariant Feature Transformation *(SIFT)* is a method used for image matching and recognition [28]. This SIFT method was widely used in computer vision related to object recognition task [29]. It was well suited for performing image matching and object recognition in real-world conditions [30]. The following were the main stages of computing used to generate the feature set of the image [31]:

- Scale-space extrema detection: It was the first stage of the computation searches for all scales and locations of the image. This was applied efficiently by using the Gaussian difference function to identify potential points of interest that were invariant to scale and orientation by using the following Equation 1:

$$L(x, y, \sigma) = G(x, y, \sigma) * \mathrm{I}(x, y) \quad (1)$$

- Key point localization: At each location candidate, a detailed model was suitable for determining location and scale. The key points were selected based on their stability measures which can be formulated as follows Equation 2:

$$D(x) = D + \frac{\partial D^T}{\partial x} x + \frac{1}{2} x^T \frac{\partial^T D}{\partial x^2} x \quad (2)$$

- Orientation assignment: One or more orientations were assigned to each key point location based on the direction of the local image gradient. All subsequent operations were performed on the transformed image data, taking into account the orientation, scale, and location parameters assigned to each feature, thereby ensuring invariance to these transformations. This process can be formulated as follows Equation 3:

$$m(x, y) = \sqrt{(L(x+1, y) - L(x-1, y))^2 + (L(x+1, y) - L(x-1, y))^2}$$
$$\theta(x, y) = tan^{-1}((L(x+1, y) - L(x-1, y)) / (L(x+1, y) - L(x-1, y))) \quad (3)$$

- Key point Descriptor: image gradient was measured at the scale selected for each keypoint. This was a representation that allowed for significant distortion and changes in light. This can be formulated as follows Equation 4:

$$f(\theta, x, y) = |J(x, y)| \delta(\theta - J(x, y)) \quad (4)$$

C. Testing

In this stage, a testing process was carried out on the collected data samples. The data samples tested were images. This testing process applied the Forensic Similarity and SIFT methods. The results of the testing of each of these methods would be analyzed and compared to the test results. In the testing process, it used Matlab tools to compare two methods

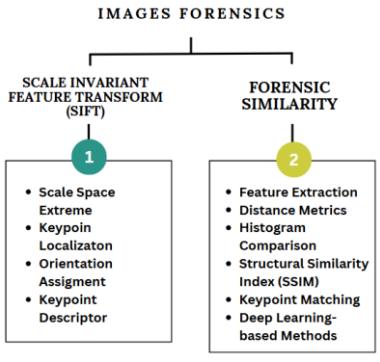


Figure 2. Method Comparison

D. Analysis

After the testing process, an analysis process was conducted to find out, compare and draw conclusions from the results of the two methods.

Results and Discussion

At this stage, the test results of two methods used in this study: the object Similarity Method and the SIFT Method. In this testing process, tests were carried out on 3 data samples. The image data used was obtained from taking pictures

with three different mobile devices: Oppo A57, Oppo A87, and Samsung SM-A525F. The meta data of the image can be seen in **Table 1**.

Table 1. Image metadata

Device	Image Name	Metadata
OPPO A57	Image1.jpg	Image Width: 3120, Image Length : 4160, Brand: OPPO, Model: OPPO A57
OPPO A87	Image2.jpg	Image Width: 6144, Image Length: 8160, Image Brand: OPPO, Model: OPPO A78
Samsung SM-A525F	Image3.jpg	Image Width : 4624 , Image Length: 3468, Brand: Samsung , Model: SM-A525F

A. Application of the Scale Invariant Feature Transform (SIFT) Method

In the application of the SIFT method applied several steps: Scale Space Extreme Detection, Localization Key point, Orientation Assumptions and Key point Descriptors [32] . This feature extraction process was carried out to compare different image descriptors to find a suitable feature.

- *Scale Space Extreme Detection*

In this Scale Space Extreme process, the potential key point location from various scales was identified using the Gaussian function. The images were blurred to generate multiple frames. This enabled key point extraction. The results of each tested image can be seen in several blur image frames as in **Figure 3**.

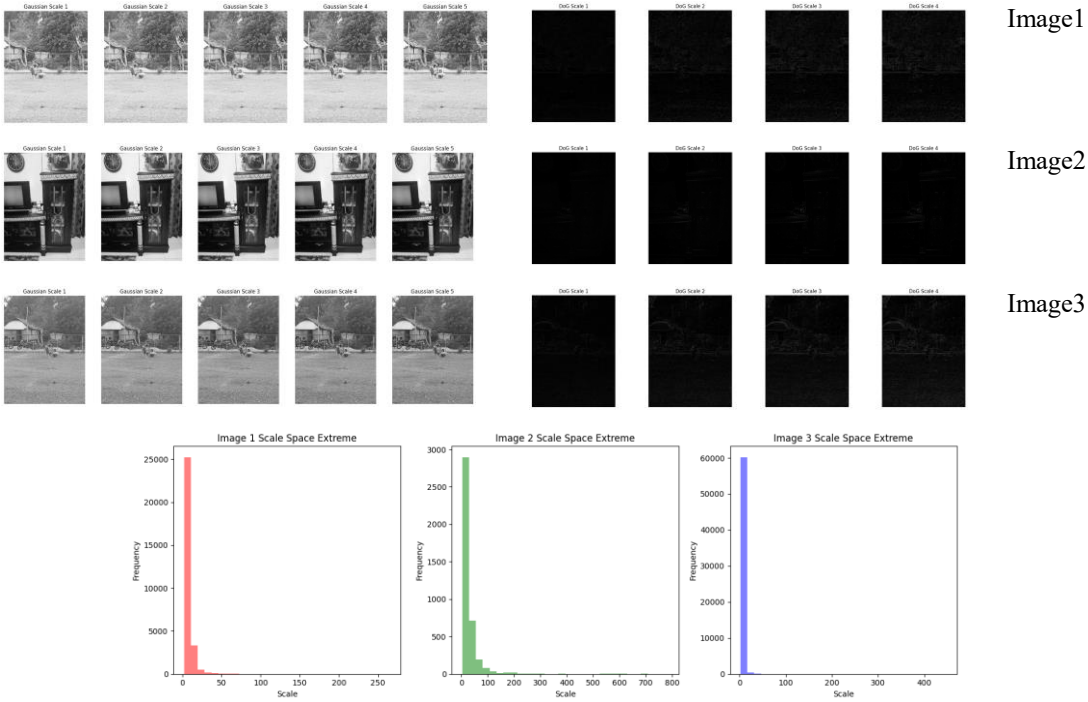


Figure 3. Results of scale space extream

In the **Figure 3** shows the difference in the distribution of the key points from each image. The value of the keypoints in this process was generated by comparing each point of the image with its 26 neighboring points. It also shows variations in the complexity of an image. The diagram above also shows that image2 has significant The next process was to find the key point value of the image. variation in the complexity of its values.

- *Key point Localization*

The next process was to find out the key point value of the image. A high key point value indicated greater amount of information that can be extracted from the image. The results of the keypoint detection in the data sample in figure 4 showed that image3 had a greater keypoint value than image1 and image2.

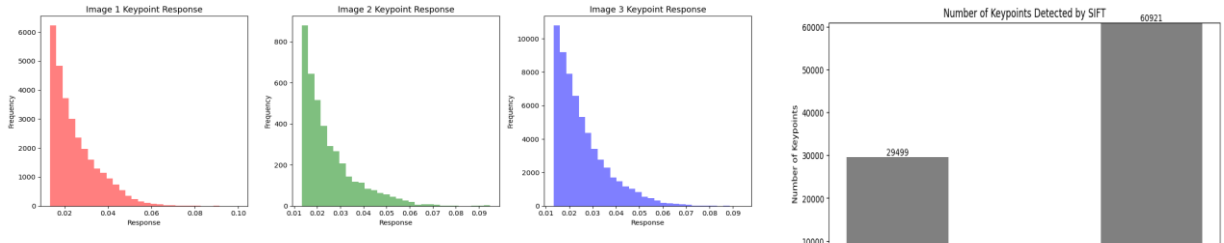


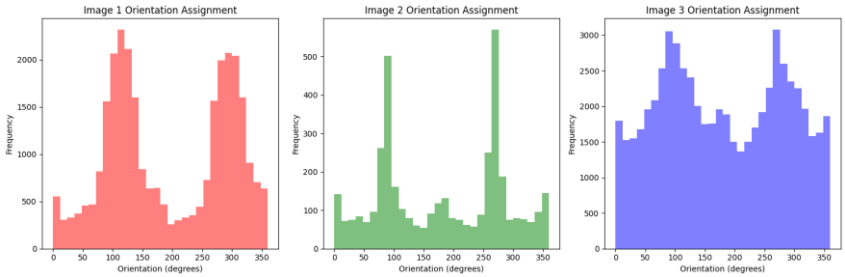
Image 1 Image 2 Image 3

Key points: 29,509 *Key points*: 4,016 *Key points*: 60,972

Figure 4. Results of Keypoint Localization

- *Orientation Assigment*

This orientation assessment process aims to understand the dominant rotation on the keypoints. This process was to determine the dominant orientation around each keypoint. As shown in **Figure 5**, the results of the data test show that the most prominent key point orientation was in image3. This is because image3 has a highest keypoin*t* value so that there is a thickness in the graph result.



Descriptors Shape: (29,509. 128) Descriptors Shape: (4,016. 128) Descriptors Shape: (60,972.128)

Figure 5. Orientation Assessment Results

- *Key point Descriptor*

The key point descriptor process was used to identify each keypoint. This process identified the pixel intensity patterns around the keypoints.

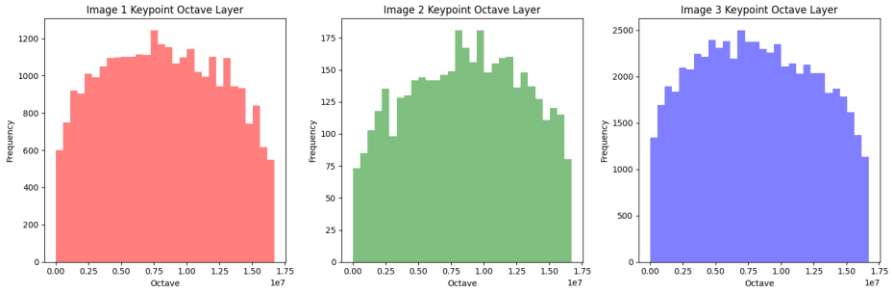


Figure 6. Descriptor keypoint results

After the four processes above, then a feature matching process was carried out to detect similarities from the tested data samples. Based on the results of the tests carried out, image 1 and image three indicated higher similarity values. As seen in the image, image1 and image3 had a high keypoint value of 3: 11,366 matches compared to image1 and image2 or image2 and image3.

- Matching between Image 1 and Image 2: 1,676 matches
- Average distance: 254.33
- Matching between Image 1 and Image 3: 11,366 matches
- Average distance: 256.71
- Matching between Image 2 and Image 3: 1,750 matches
- Average distance: 255.83

Figure 7. Results of Feature Matching

B. Application of Forensic Similarity Method

In object similarity, mapping of image patch pairs was carried out to obtain scores that contained the same or different forensic trace information to make forensic decisions. This process used two CNN models, namely based feature extractor and three-layer neural network. There were 6 stages at this stage as follows:

- *Feature Extraction*

In the Forensic Similarity, the first step was a feature extraction on the image to be sampled. Feature extraction aimed to identify similarities and differences in the image. Based on the graph shown in **Figure 7**, there is a keypoints which shows the variation in the size of the detected feature in the image. The angular key point indicated the orientation of the detected feature in the image.

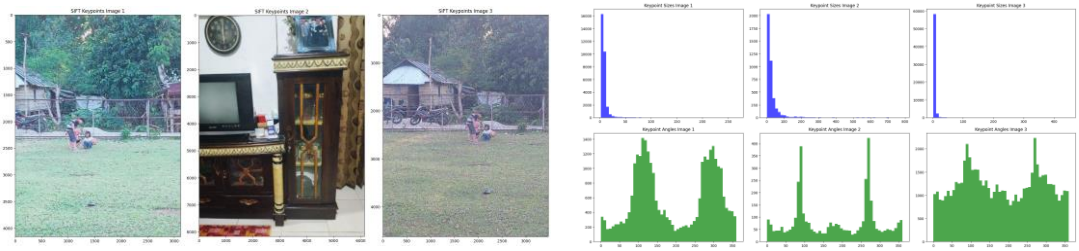


Figure 8. Feature Extraction Results

From the results of the test carried out as shown in **Table 2**, the size of the keypoint indicates that image1 and image 3 have very large keypoint and descriptor values compared to image2. This showed that the image1 and image3 pads have a lot of information that can be extracted.

Table 2. Fiture Extraction results table

Image 1	Image 2	Image 3
Number of *Keypoints*: 29,509 Descriptors Shape: (29,509.128)	Number of *Keypoints*: 4.016 Descriptors Shape: (4.016.128)	Number of *Keypoints*: 60,972 Descriptors Shape: (60,972.128)

- *Distance Metrics*

The Distance matrix process was to calculate the distance of each image. The process of calculating the distance of each of these images was carried out by calculating the Euclidean, Manhattan, and Cosine distances between the descriptors of each pair of images to obtain the average distance between the extracted features.

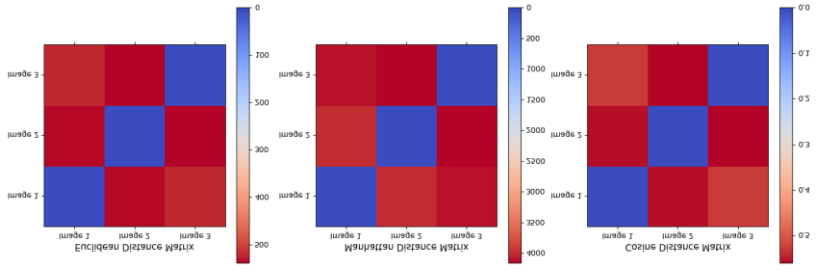


Figure 9. Distance Metrics Results

From the test results conducted based on the table of 3, the smaller values show that the features of the two images have proximity to each other. This can be seen in the values of the Euclidean Distance in image1 and image3. Then the Manhattan Distance values of image1 and image2 have greater similarity because they have the smallest Manhattan Distance values. As for the Cosine Distance value, image2 and image3 have a greater similarity because the Cosine Distance value is close to 1.

Table 3. Distance metrics results

Euclidean Distance	Manhattan Distance	Cosine Distance
• Distance between Image 1 and Image 2: 535.8839 • Distance between Image 1 and Image 3: 522.2203 • Distance between Image 2 and Image 3: 539.4870	• Distance between Image 1 and Image 2: 3,993.6730 • Distance between Image 1 and Image 3: 4,113.4277 • Distance between Image 2 and Image 3: 4,163.3037	• Distance between Image 1 and Image 2: 0.5545 • Distance between Image 1 and Image 3: 0.5259 • Distance between Image 2 and Image 3: 0.5608

- *Histogram Comparison*

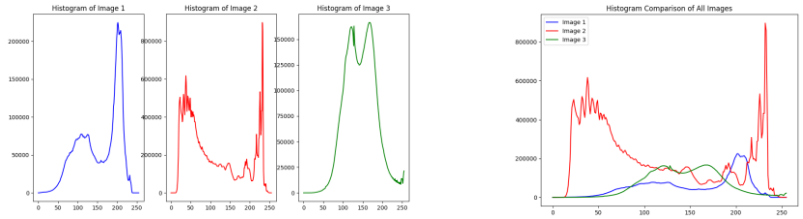


Figure 10. Histogram Comparison Results

The histogram comparison process was used to analyze the differences from the image through the image histogram. This color histogram represented the distribution of pixel intensity based on the Wana value in the image. In the detection of histogram comparison, there were 4 assessed components: Correlation, Chi-Square, Intersection, and Bhattacharyya.

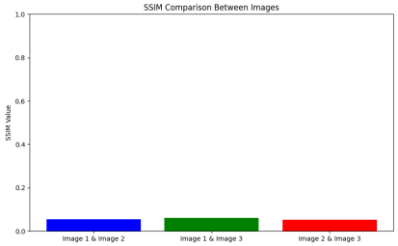
Table 4. Chart of histogram comparison results

Comparison between Image 1 and Image 2:	Comparison between Image 1 and Image 3:	Comparison between Image 2 and Image 3:
• Correlation: -0.24750548829748123 • Chi-Square: 3114823370.902912 • Intersection: 11151496.0 • Bhattacharyya: 0.47656070690751823	• Correlation: 0.27319050488938373 • Chi-Square: 48597578.864574715 • Intersection: 8321226.0 • Bhattacharyya: 0.3474037420740563	• Correlation: -0.39486202482239563 • Chi-Square: 85084689.32834741 • Intersection: 13502826.0 • Bhattacharyya: 0.5524044481953799

Correlation values of 1 indicated identical histograms, while values of -1 indicated very different histograms. Chi-Square values that had lower values indicated more similar histograms, Intersection values measured overlapping histograms with higher values indicating similar histograms. Bhattacharyya's value measured the difference between two histograms with low values showing more similar histograms.

- *Structural Similarity Index (SSIM)*

The Structural Similarity Index (SSIM) measured the similarity between two images. SSIM values range from -1 to 1, where a value of 1 indicated a perfect similarity between two images, while a lower value indicated more structural differences between images. From the results of the data and graphs obtained from the test, it can be seen that the comparison between image1 and image 2, as well as image2 and image3 had a lower *S*tructural Similarity Index value than image1 and image3. This shows that image1 and image3 had a Structural Similarity Index.



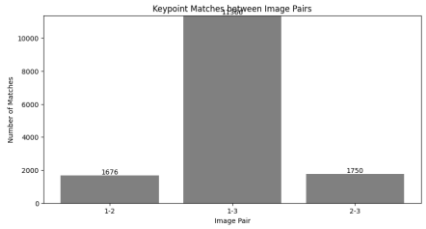
- SSIM between image 1 and image 2: 0.0538
- SSIM between image 1 and image 3: 0.0613
- SSIM between image 2 and image 3: 0.0529

Figure 11. Results of the Structural Similarity Index (SSIM)

- ***Keypoint Matching***

In the keypoint matching, an indication of the similarity of the two images was presented. The more the picture match, the more similar the images are. From the results of the test carried out, image1 and image3 has the highest

number of matches. This indicates that image1 and image3 have greater similarities and have greater structural similarities.

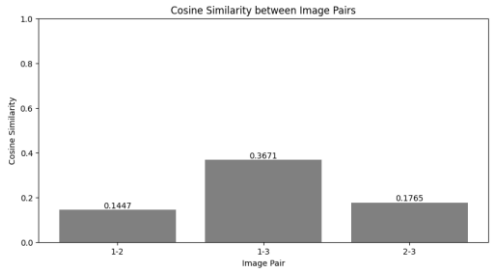


- Number of matches between Image 1 and Image 2: 1,676
- Number of matches between Image 1 and Image 3: 11,366
- Number of matches between Image 2 and Image 3: 1,750

Figure 12. Keypoint Matching Results

▪ *Deep Learning-based Methods*

This process was carried out to find the value of Cosine Similarity. Cosine similarity identified similarities between two feature vectors extracted by the deep learning model. The Cosine similarity value ranged between -1 and 1, with higher values indicating greater similarity. From the results of the data testing carried out, it can be concluded that the Cosine similarity between image1 and image3 had the largest value. This shows that image1 and image3 had greater similarities in their extracted features.



- Cosine similarity between Image 1 and Image 2: 0.1447
- Cosine similarity between Image 1 and Image 3: 0.3671
- Cosine similarity between Image 2 and Image 3: 0.1765

Figure 13. Results of Deep Learning-based Methods

C. Analysis

Based on the results of testing data samples using the SIFT method and the Forensic Similarity Method , forensic images can be applied to forensic images by looking for similarities of image objects. In the *SIFT* method, the process of detecting similarities in forensic images can be carried out in 4 stages: scale space extreme, localization key points, orientation assessment, and key point descriptor. The process was conducted by using a Gaussian function on the image by turning the image into blur in several frames. This was to find the keypoint value of each image. This keypoint search process was carried out to extract information in the image. The higher the keypoint value of an image, the more information is in the image. Next, the orientation assessment process was carried out to search for the most prominent key point orientation from the existing data sample and lastly a descriptor key point process was carried out to identify each key point value based on the pixel intensity pattern around the keypoint.

Meanwhile, in the object similarity method there were 6 stages to detect the similarity of the image object: feature extraction, distance metrics, histogram comparison, Structural Similarity Index *(SSIM),* key point matching and Deep Learning-based methods. The feature extraction process was carried out to identify the features in the image to detect similarities. This process looked for variations in feature size by measuring the size of keypoints and the angle of keypoints. Next, a distance matrix process was carried out to calculate the average distance between the extracted features by searching for Euclidean, Manhattan, and Cosine values. Furthermore, the histogram comparison process was conducted for the analysis of pixel intensity distribution based on Wana values. The process was carried out through Correlation, Chi-Square, Intersection, and Bhattacharyya analyses for the similarity detection. The Structural Similarity Index (SSIM) process was also employed to measure the similarity between two images based on the SSIM values. A value of 1 indicated an identical histogram, while a value of -1 indicated a very different histogram. The keypoint matching process was also carried out to identify the number of keypoints in the image. *The high keypoint* values of the two images indicated the similarity of the images. The last step taken was Deep Learning-based Methods to find the Cosine Similarity value where the higher value indicated greater similarity between two images.

Conclusion

This study aimed to compare two methods in forensic image identification. The results showed that these two methods can be utilized for the forensic image process. The SIFT method performs forensic image identification by detecting the similarity of images by calculating the key point value of each image. The search process for this keypoint was carried out to obtain image extraction. *A* high keypoint value indicates the high amount of information obtained from image extraction. Meanwhile, the Similarity Forensic Method also detects forensic images by looking at image patches to see if they have the same forensic traces. The advantage of the Forensic Similarity method compared to the SIFT method is that Forensic Similarity produces more detailed than SIFT because its process involves many processes so that it can identify similarities between two image patch objects. In addition, the results obtained from the Forensic Similarity method are more detailed in detecting image similarity by looking at the keypoint matching and Cosine Similarity values. Several previous studies have been conducted in the implementation of SIFT and Forensic Similarity methods for image forensics, but there has been no research that directly compares these two methods. This is the uniqueness of this research. However, this study only used three data samples from three different devices for data collection. For the development of future research, many data samples can be used to see the results of comparison and testing with actual forensic scenarios.

References

[1] Manisha, A. K. Karunakar, and C. T. Li, "Identification of source social network of digital images using deep neural network," *Pattern Recognit Lett*, vol. 150, pp. 17–25, Oct. 2021, doi: 10.1016/j.patrec.2021.06.019.

[2] P. Sharma, M. Kumar, and H. K. Sharma, "GAN-CNN Ensemble: A Robust Deepfake Detection Model of Social Media Images Using Minimized Catastrophic Forgetting and Generative Replay Technique," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 948–960. doi: 10.1016/j.procs.2024.04.090.

[3] M. Fakhrulddin Abdulqader, A. Y. Dawod, and A. Zeki Ablahd, "Detection of tamper forgery image in security digital mage," *Measurement: Sensors*, vol. 27, Jun. 2023, doi: 10.1016/j.measen.2023.100746.

[4] I. C. Camacho and K. Wang, "A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics," *J Imaging*, vol. 7, 2021.

[5] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A survey of machine learning techniques in adversarial image forensics," *Comput Secur*, vol. 100, p. 102092, 2021, doi: 10.1016/j.cose.2020.102092.

[6] K. B. Meena and V. Tyagi, "A copy-move image forgery detection technique based on tetrolet transform," *Journal of Information Security and Applications*, Vol. 52, p. 102481, 2020, doi: 10.1016/j.jisa.2020.102481.

[7] M. Jafari Barani, M. Yousefi Valandar, and P. Ayubi, "A new digital image tamper detection algorithm based on integer wavelet transform and secured by encrypted authentication sequence with 3D quantum map," *Optics (Stuttg)*, vol. 187, pp. 205–222, Jun. 2019, doi: 10.1016/j.ijleo.2019.04.074.

[8] S. K. Sharma, A. AlEnizi, M. Kumar, O. Alfarraj, and M. Alowaidi, "Detection of real-time deep fakes and face forgery in video conferencing employing generative adversarial networks," *Heliyon*, Vol. 10, No. 17, p. E37163, 2024, doi: 10.1016/j.heliyon.2024.e37163.

[9] G. G. Rajput, S. D. Dabhole, and Prashantha, "Modified Keypoint-Based Copy Move Area Detection," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 3389–3396. doi: 10.1016/j.procs.2024.04.319.

[10] B. Wang, J. Hou, F. Wei, F. Yu, and W. Zheng, "MDM-CPS: A few-shot sample approach for source camera identification," *Expert Syst Appl*, vol. 229, Nov. 2023, doi: 10.1016/j.eswa.2023.120315.

[11] A. Akilal and M. T. Kechadi, "An improved forensic-by-design framework for cloud computing with systems engineering standard compliance," *Forensic Science International: Digital Investigation*, vol. 40, Mar. 2022, doi: 10.1016/j.fsidi.2021.301315.

[12] N. B. A. Warif *et al.*, "Copy-move forgery detection: Survey, challenges and future directions," *Journal of Network and Computer Applications*, vol. 75, pp. 259–278, 2016, doi: 10.1016/j.jnca.2016.09.008.

[13] F. Breitinger, X. Zhang, and D. Quick, "A forensic analysis of rclone and rclone's prospects for digital forensic investigations of cloud storage," *Forensic Science International: Digital Investigation*, vol. 43, Sep. 2022, doi: 10.1016/j.fsidi.2022.301443.

[14] Y. Zhou *et al.*, "Digital whole-slide image analysis for automated diatom test in forensic cases of drowning using a convolutional neural network algorithm," *Forensic Sci Int*, vol. 302, Sep. 2019, doi: 10.1016/j.forsciint.2019.109922.

[15] O. Mayer and M. C. Stamm, "Forensic Similarity for Digital Images," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1331–1346, 2020, doi: 10.1109/TIFS.2019.2924552.

[16] G. G. Rajput, S. D. Dabhole, and Prashantha, "Modified Keypoint-Based Copy Move Area Detection," *Procedia Comput Sci*, vol. 235, pp. 3389–3396, 2024, doi: 10.1016/j.procs.2024.04.319.

[17] J. Guo, H. Chen, B. Liu, and F. Xu, "A system and method for person identification and positioning incorporating object edge detection and scale-invariant feature transformation," *Measurement (Lond)*, vol. 223, Dec. 2023, doi: 10.1016/j.measurement.2023.113759.

[18] E. Akbal and S. Dogan, "Forensics Image Acquisition Process of Digital Evidence," *International Journal of Computer Network and Information Security*, vol. 10, no. 5, pp. 1–8, 2018, doi: 10.5815/ijcnis.2018.05.01.

[19] V. Vijayan and P. Kp, "A Comparative Analysis of RootSIFT and SIFT Methods for Drowsy Features Extraction," in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 436–445. doi: 10.1016/j.procs.2020.04.046.

[20] M. Yacoub, M. Abdelwahab, K. Shiokawa, and A. Mahrous, "Estimating the drift velocity of plasma bubbles in airglow images using the scale invariant feature transform and the speeded up robust feature algorithms," *Advances in Space Research*, 2024, doi: 10.1016/j.asr.2024.09.071.

[21] F. Marra, Di. Gragnaniello, L. Verdoliva, and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," *IEEE Access*, vol. 8, pp. 133488–133502, 2020, doi: 10.1109/ACCESS.2020.3009877.

[22] G. Horsman, "Defining principles for preserving privacy in digital forensic examinations," *Forensic Science International: Digital Investigation*, vol. 40, Mar. 2022, doi: 10.1016/j.fsidi.2022.301350.

[23] J.-Y. Sun, S.-W. Kim, S.-W. Lee, and S.-J. Ko, "A novel contrast enhancement forensics based on convolutional neural networks," *Signal Process Image Commun*, vol. 63, pp. 149–160, 2018, doi: 10.1016/j.image.2018.02.001.

[24] B. Bayar and M. C. Stamm, "Towards Open Set Camera Model Identification Using a Deep Learning Framework," *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*Pp. 2007–2011, 2018.

[25] O. Mayer and M. C. Stamm, "Learned Forensic Source Similarity for Unknown Camera Models," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Apr. 2018, pp. 2012–2016. doi: 10.1109/ICASSP.2018.8462585.

[26] B. Bayar and M. C. Stamm, "On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2017, pp. 2152–2156. doi: 10.1109/ICASSP.2017.7952537.

[27] J. Bunk *et al.*, "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning," in *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 2017, pp. 1881–1889. doi: 10.1109/CVPRW.2017.235.

[28] Y. Sun, "Exploration on Data Collection and Analysis System Based on Integrated SIFT Algorithm," in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 388–395. doi: 10.1016/j.procs.2024.09.048.

[29] S. Arooj, S. Altaf, S. Ahmad, H. Mahmoud, and A. S. N. Mohamed, "Enhancing sign language recognition using CNN and SIFT: A case study on Pakistan sign language," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 2, Feb. 2024, doi: 10.1016/j.jksuci.2024.101934.

[30] T. Lindeberg, "Image Matching Using Generalized Scale-Space Interest Points," *J Math Imaging Vis*, vol. 52, no. 1, pp. 3–36, May 2015, change: 10.1007/s10851-014-0541-0.

[31] L. Daoud, M. K. Latif, H. S. Jacinto, and N. Rafla, "A fully pipelined FPGA accelerator for scale invariant feature transform keypoint descriptor matching," *Microprocess Microsyst*, vol. 72, Feb. 2020, doi: 10.1016/j.micpro.2019.102919.

[32] T. P. Shiji, S. Remya, and V. Thomas, "Computer Aided Segmentation of Breast Ultrasound Images Using Scale Invariant Feature Transform (SIFT) and Bag of Features," in *Procedia Computer Science*, Elsevier B.V., 2017, pp. 518–525. doi: 10.1016/j.procs.2017.09.108.