



IMAGE FORENSICS USING ERROR LEVEL ANALYSIS AND BLOCK MATCHING METHODS

¹Iis Sudianto, ²Nuril Anwar,

¹Informatics Departement, Universitas Ahmad Dahlan Yogyakarta, Indonesia

²Informatics Departement, Universitas Ahmad Dahlan Yogyakarta, Indonesia

e-mail: iissudianto@gmail.com, nuril.anwar@tif.uad.ac.id

Abstract

The development of image editing tools today makes everyone able to manipulate images easily so that many images are doubtful of their authenticity. The current image can be used as evidence in a legal case in court. The authenticity of the image is a topic that many have tried to solve various studies. This study discusses the authenticity of the image using the Error Level Analysis (ELA) method to determine the authenticity of the image, especially in the JPEG image. Block Matching is used in the process of dividing an image into several square or block parts. The ELA method has been successfully implemented with 95% image compression resulting in MSE and PSNR values in distinguishing the edited image. The average MSE is 23.8 dB and the average PSNR is 34.47 dB. Block Matching results as a whole show that the pixel value for x values that reach 30 there are 9 images, x values that reach 24 there are 9 images, x values that reach 23 there are 1 image, and for x values that reach 19 there is 1 image. The result of pixel (y) of all images exceeds the value of 12 which in pixel (y) undergoes many changes marked by the presence of white spots.

Keywords : *Block Matching, ELA, Forensics Image, Error Level*

INTRODUCTION

Technological developments can have both positive and negative impacts. The positive impact is that it can help complete difficult work, while the negative impact is the number of crime cases using technology in the field of image editing. Crime in technology is called cybercrime[1]. Cybercrime is a crime related to the use of information and communication technology, and has strong characteristics with technology and communication engineering that relies on a high level of security and information submitted and accessed by internet users[2].

Technological developments in digital image processing make it easier for users to fake images[3]. The impact of image falsification is the creation of a new image that is different from the original[4]. This can lead to misunderstandings for someone who sees the image, so that the image is difficult to distinguish whether it is still original or has been modified. Then the image can be easily and quickly spread, then it can cause controversy and can become a crime.

In general, a false image can be said to be a fraud, although not all false images are bad things that can be used as entertainment, they can even be used for research purposes[5], for example problems related to understanding the quality of an image[6]. However, these actions can be called evil and dangerous when creating a false image for profit.

Due to the ease of manipulating the image, someone who sees the image becomes hesitant to believe the authenticity of the image that is spread on social media[7]. Then to avoid this, a step is needed that can provide certainty to the authenticity of an image. Thus, it is important for someone to have knowledge that an image has been manipulated or not, so we need a technique that can analyze the changes that have occurred in the image. To prove the authenticity of an image, it is tested using the JPEGsnoop software.

The method used in this research is the Error Level Analysis and Block Matching method[8]. Error Level Analysis is a method to find out whether there are modifications or not in an image,

especially in JPEG images, because in general, images circulating on the internet are images with JPEG format. Meanwhile, Block Matching is the process of dividing the image into several square or block parts[9]. However, the Error Level Analysis method requires additional tools to provide a label in the form of a block to identify the results of the Error Level Analysis extraction, so the Block Matching method is used as a tool to help read the results of the Error Level Analysis[10]. Therefore, this research raises the title of the final project entitled "Image Forensics Analysis Using Error Level Analysis and Block Matching Methods".

THEORETICAL BASIS

A. Previous Research

According to[11], discussing image manipulation, currently many people can manipulate images without leaving a trace on the image that has been manipulated so that many scattered images are doubtful of authenticity, because images can be used as evidence in legal cases. By using several methods applied in this research, such as the Error Level Analysis (ELA) method, which is a very good method for reading image forgery with the help of the Block Matching method so that the results become more accurate and efficient.

According to[12], discussing Image Forensics which explains the development of digital imaging technology. This has led to the extensive use of digital images for various purposes, but digital images are often manipulated to lose the authenticity of the image. As a result, digital images are difficult to trust by the public. This study analyzes the error rate using the ELA technique for passive authentication in image forensics which involves JPEG compression, image splicing, copyrighted image engineering and image retouching, then uses compression and resizing techniques.

According to[13], discussing Photo Counterfeit Detection Using Image Forensics that advances in editing software make images easy to manipulate, image changes can be edited easily, so that original information can be changed and can be used for criminal acts. The purpose of this study is to obtain evidence of truth in determining the authenticity of the image with several methods. With the Error Level Analysis method and the help of tools that can provide detection information from the image. The comparison of the three tools was successfully carried out with each analysis that was already running, so that the image detection results were obtained.

According to[14], discussing copy-move that more and more people easily modify images which have an impact on image falsification. Image forgery can cause misunderstanding for someone who sees the image. Someone who sees it has difficulty in distinguishing the image is an original image or a modified one. The Block Matching method with both approaches will be compared to find out which one is better at detecting copy-move.

According to[11], discussing the detection of image modifications that forgery is difficult to determine its authenticity. Cases of image modification that occur, for example, there is the emergence of a modified digital image that causes problems in social media such as the spread of false information, so that it is easy for misunderstandings to occur. With the help of the Error Level Analysis method, you can detect image modifications by analyzing the image using editing software.

Forensics Image

Image Forensics is a branch of multimedia security that aims to distinguish image manipulation by criminals[15]. The goal is to support the investigation and be assisted with tools related to evidence. Processing tools used in analysis such as watermarking and steganography, both of which can assist in recovering image information. Both of these processing tools are commonly known as digital image forensics.

JPEG Image

JPEG is the format used for photographic images. The JPEG format uses the extension (.jpeg, .jpg, .jpe, .jfif, .jif). JPEG is also useful in creating high-quality images with small file sizes, so this format is an alternative that can be used to obtain satisfactory image results[16].

JPEGSnoop

JPEGSnoop is a tool that can help detect whether a photo has been manipulated or is still original. JPEGSnoop is able to detect various settings used in a digital camera (EXIF metadata, IPTC) and can also compare a photo with many compression parameters. These parameters vary, depending on the type of camera or software used.

RESEARCH METHODS

A. Error Level Analysis

This Error Level Analysis technique is used to detect digitally modified images. The concept of the ELA method is a technique with JPEG images undergoing double compression, double compression or so-called Ghost JPEG techniques. The flow of the method is shown in Figure 1



Fig. 1 Error Level Analysis Method Flow

Based on the flow of the ELA method, the image results in the form of a true color (RGB) image will be obtained, then the results of the ELA will look for the difference in the values of the two images by comparing the PSNR values. Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum values of the two images. PSNR is measured in decibels. In this study, PSNR is used to compare the quality of image 1 before and image 2. To determine PSNR, MSE must first be determined. The lower the MSE value, the better, and the larger the PSNR value, the better the image quality, and conversely, the higher the MSE value, the more visible it is that there is editing on the image and the smaller the PSNR value, the more visible it is that there is editing on the image.

B. Block Matching

The Block Matching method is a method that can be used to detect the copied region[17]. This block is first placed in the top left corner and moves one pixel and then down. The pixels are picked up by the column in each block position and placed into the matrix. matrix will have columns and rows. The matrix is then searched with respect to the same rows but corresponding to different regions of the image, thereby indicating that a portion

of the image has been copied from one location to another. The following is an explanation of the Block Matching technique in Figure 2

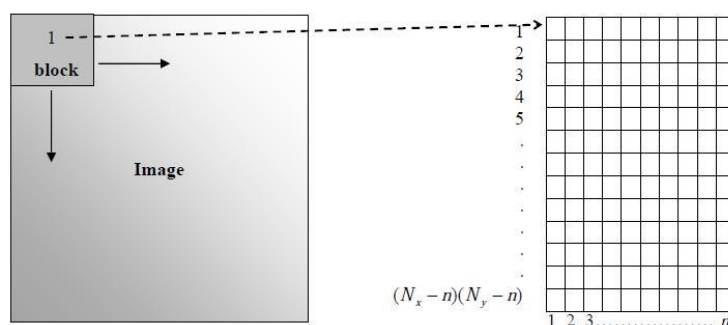



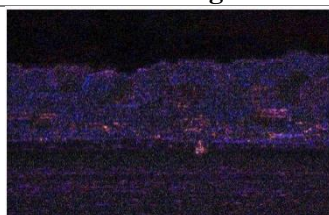
Fig. 2 Block Matching Method

This technique follows the running time according to the desired size of the $B \times B$ block. The block size also determines the desired accuracy of the drawing. This technique encourages detecting copy-move forgery, but when viewing JPEG images one should be aware that due to low compression many objects that were not actually manipulated will be detected as well. The Block-Matching method is highly recommended to reduce computation time. In the matching procedure, the image is divided into two blocks, the first block is considered overlapping, and then all pairs of duplicate blocks will be marked[18].

RESULTS AND DISCUSSION

In the Error Level Analysis JPEG image technique, this is done to identify the parts of the compression. Error Level Analysis technique can be used to determine an original image with a digitally modified image. The working concept of the Error Level Analysis method is that an image is divided into 8×8 blocks and compressed again at an image error level of 95%. The detection process in Error Level Analysis begins with creating a scenario in the form of preparing two image files from two different sources. The following is an image of the results of the Error Level Analysis method shown in Table 1. The results of Error Level Analysis

Table 1 Error Level Analysis Result

Image 1	Image 2
	
Image_Name : beach_1	Image_Name : beach_2

The process results from the Error Level Analysis will then be calculated to find the MSE and PSNR values using Gaussian noise reduction by converting the ELA results to grayscale. Meanwhile, the filter used to restore the two images uses a 3×3 kernel. Then these parameters are used as an indicator to compare the results of processing 2 (two) images. The following is the result value of the three parameters by comparing 2 (two) images contained in Figure 3 Parameter Result Value for MSE and PSNR beach_1. The process of obtaining the result

values of MSE and PSNR using Gaussian noise reduction. Based on image data sample 1, it produces MSE: 24.6574 and PSNR: 34.2453. Furthermore, an experiment was carried out on image data sample 2, which is shown in Figure 4. Result Value of beach_2 Parameters.

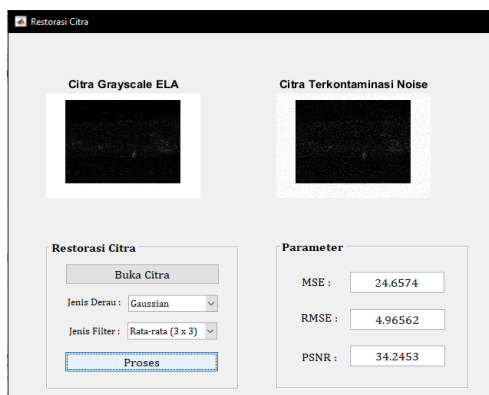


Fig. 3 MSE and PSNR Result Value beach_1

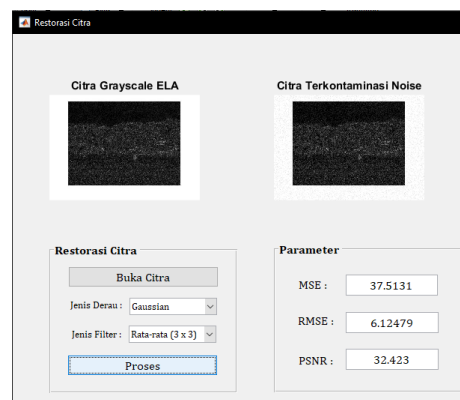



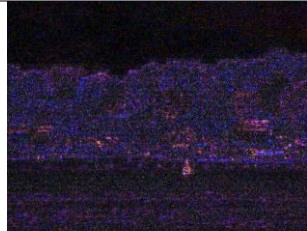


Fig. 4 MSE and PSNR Result Value beach_2

Based on the sample data, image 2 produces MSE: 37,5131 and PSNR: 32,423. From the test results of 2 (two) eating images, the difference between the two images contained in the ELA Test Results Table calculates the MSE and PSNR Values.

Table 2 ELA Test Results Calculating MSE and PSNR Nilai Values

Image Name	Compression ELA (95%)	MSE and PSNR	Keterangan
 beach_1		MSE : 24.6574 PSNR : 34.2453	The results of the MSE values of the two images show that image 2 has a larger MSE value and a smaller PSNR value than image 1, so it can be concluded that image 2 is an image that has been edited.
 beach_2		MSE : 37.5131 PSNR : 32.423	

Based on the results of the MSE values of the two images, it shows that beach_2 has a larger MSE value and has a smaller PSNR value than beach_1, so it can be concluded that beach_1 is the original image and beach_2 is an image that has been edited, because the lower the MSE value, the more good, and the greater the PSNR value, the better the image quality, and conversely, the higher the MSE value, the more visible it is that there is editing on the image and the smaller the PSNR value, the more visible it is that there is editing on the image. The calculation process to find the MSE and PSNR values uses Gaussian noise reduction by converting the ELA results to grayscale using a 3 x 3 kernel to rotate the two images. Then

these parameters are used as indicators to compare the results of processing 2 (two) images, where the lower the MSE value, the better, and the greater the PSNR value, the better the image quality, and conversely, the higher the MSE value, the more visible it is that there are editing on the image and the smaller the PSNR value, the more visible it is that there is editing on the image. The following is Table 3 ELA Test Results MSE and PSNR

Table 3 ELA MSE and PSNR Result Values

Image Name	MSE	PSNR	Image Name	MSE	PSNR
bdg_1	25.22	34.14	mangga_1	18.34	35.53
bdg_2	25.45	34.10	mangga_2	18.74	35.43
beach_1	24.65	34.24	motor_1	20.51	35.04
beach_2	37.51	32.42	motor_2	19.77	35.2
becak_1	21.73	34.79	mount_1	19.07	35.35
becak_2	22.72	34.6	mount_2	18.93	35.39
bridge_1	25.83	34.04	padat_1	31.42	33.19
bridge_2	27.09	33.83	padat_2	32.22	33.08
cake_1	21.73	34.79	pohon_1	26.13	33.99
cake_2	21.92	34.75	pohon_2	26.97	33.85
danau_1	17.43	35.74	sepeda_1	21.41	34.85
danau_2	16.84	35.89	sepeda_2	20.42	35.06
gedung_1	27.79	33.72	street_1	25.22	34.4
gedung_2	27.86	33.71	street_2	22.75	34.59
hutan_1	26.99	33.69	streetfood_1	24.65	34.24
hutan_2	26.00	33.85	streetfood_2	23.83	34.39
langit_1	16.01	36.12	tangga_1	20.71	35
langit_2	15.93	36.14	tangga_2	22.74	34.5
mall_1	21.44	34.85	tugu_1	20.69	35
mall_2	21.46	34.84	tugu_2	19.60	35.2

Based on the results of the calculation of the MSE and PSNR values using 20 sample images, it is found that there is editing in one of the marked images in Table 4 Average Results of MSE and PSNR ELA.

Table 4 Average Result of MSE and PSNR ELA

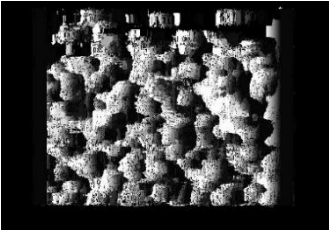
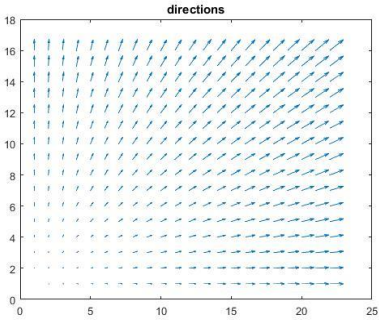
Image Name	MSE (dB)	PSNR (dB)
bdg_2	25.45	34.10
beach_2	37.51	32.42
becak_2	22.72	34.6
bridge_2	27.09	33.83
cake_2	21.92	34.75
danau_1	17.43	35.74
gedung_2	27.86	33.71
hutan_1	26.99	33.69
langit_1	16.01	36.12
mall_2	21.46	34.84
mangga_2	18.74	35.43
motor_1	20.51	35.04
mount_1	19.07	35.35
padat_2	32.22	33.08
pohon_2	26.97	33.85

sepeda_1	21.41	34.85
street_1	25.22	34.4
streetfood_1	24.65	34.24
tangga_2	22.74	34.5
tugu_1	20.69	35
Mean	23.8 dB	34.47 dB

From table 4.7 above, it can be seen that the average MSE value is 23.8 dB and the average PSNR value is 34.47 dB, this shows that image editing has been successfully proven, because the success of a method can be known if the MSE value is low and the PSNR value is high, two images have a low level of similarity if the PSNR value is below 30 dB[19].

The next detection process is carried out using the Block Matching method, this method helps read the compression results from Error Level Analysis to detect image manipulation by giving blocks to suspected areas. In this process, two image files are prepared as a result of compression from Error Level Analysis, which are then both images. The block taking stage is shifted every one pixel in all parts of the image from the top left corner to the bottom right corner in order to the right and then down[20]. Each image is divided into blocks based on sub-regions and the differences in each block will be found. This sorting process can shorten the search time of all blocks. The Block Matching method produces a black and white image that has marked differences from the two images that have been processed using Error Level Analysis and Block Matching. The results obtained are in the form of a two-dimensional direction $f(x,y)$ which has row and column sizes where x and y are the coordinates of the image and $f(x,y)$ is the light intensity (brightness) or gray level (grey level). A digital image is a matrix where the row and column indexes represent a point in the image and the matrix elements (which are referred to as image elements or pixels) represent the value of the degree of gray at that point. The following is Table 5 Test Results of the Block Matching Method

Table 4 Block Matching Method Test Results

Image Block Matching	Direction Result (x,y)
 <p style="text-align: center;">Image Name : bm_beach</p>	 <p>The second direction of the image produces a value of $x = 23$ and a value of $y = 17$.</p>

The test results in the table above are image manipulation detection using the Block Matching method. The Block Matching method produces a black and white image that has marked differences from the two images that have been processed using Error Level Analysis and

Block Matching. The results obtained are in the form of a two-dimensional $f(x,y)$ direction where the largest pixel (x,y) value in the image has the most white spots or there are many differences in the image. The following are the results of the x and y values of the Block Matching image contained in Table 4.6

Table 5 Pixel Value Result (x,y) Block Matching

Image Name	Pixel X	Pixel Y
<i>bdg</i>	30	22
<i>beach</i>	23	17
<i>becak</i>	30	23
<i>bridge</i>	24	22
<i>cake</i>	19	19
<i>danau</i>	24	22
<i>gedung</i>	24	22
<i>hutan</i>	30	22
<i>langit</i>	30	22
<i>mall</i>	24	19
<i>mangga</i>	30	20
<i>motor</i>	24	22
<i>mount</i>	24	22
<i>padat</i>	24	22
<i>pohon</i>	30	22
<i>sepeda</i>	30	20
<i>street</i>	30	23
<i>streetfood</i>	30	22
<i>tangga</i>	24	22
<i>tugu</i>	24	22

Based on the results of the pixel value (x,y) from Block Matching based on the sub region value with a length of 30 and a width of 12, this value is used to determine the pixel point in matching the two images by marking the part that has occurred editing. The following is the percentage value of Block Matching in the trial using a length value of 30 and a width of 12 which is shown in Fig. 5.

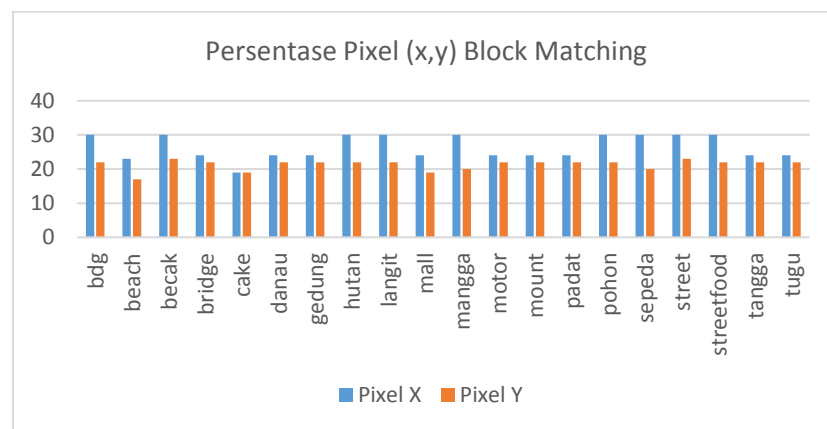


Fig. 5 Pixel Value Percentage

Based on the graph of the percentage value of the Block Matching percentage value in the trial using a length value of 30 and a width of 12, the overall results show that the pixel values for x values that reach 30 are 9 images, while for x values that reach 24 there are 9 images. x that reaches 23 there is 1 image, and for the value of x that reaches 19 there is 1 image. The percentage is the number of pixels that have been marked with white dots which indicate that the area has changed. An image whose value is close to the length value means that the pixel image has changed a lot. Then for the results of the width value in the image of 20 Block Matching data, the results show that the entire image exceeds the value of 12, where the pixel value (y) has undergone many changes, marked by white spots.

CONCLUSION

After conducting tests and analyses on image authenticity using the Error Level Analysis (ELA) and Block Matching methods, the study reached the following conclusions: The ELA method effectively detected image authenticity in JPEG files with 95% compression, producing an average MSE value of 23.8 dB and a PSNR value of 34.47 dB, distinguishing edited images. The Block Matching method supported ELA by reading compression results, showing pixel x-values of 30 in 9 images, 24 in 9 images, 23 in 1 image, and 19 in 1 image. Additionally, pixel y-values across all images exceeded 12, indicating many changes marked by white spots. Lastly, the JPEGsnoop tool provided useful information about the cameras used to capture original images.

BIBLIOGRAPHY

- [1] A. Shatté, A. Perlman, B. Smith, and W. D. Lynch, 'The Positive Effect of Resilience on Stress and Business Outcomes in Difficult Work Environments', *J. Occup. Environ. Med.*, 2017, doi: 10.1097/JOM.0000000000000914.
- [2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, 'A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications', *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2683200.
- [3] G. K. Birajdar and V. H. Mankar, 'Digital image forgery detection using passive techniques: A survey', *Digital Investigation*. 2013. doi: 10.1016/j.diin.2013.04.007.
- [4] A. N. Katsaounidou, A. Gardikiotis, N. Tspilas, and C. A. Dimoulas, 'News authentication and tampered images: evaluating the photo-truth impact through image verification algorithms', *Heliyon*, 2020, doi: 10.1016/j.heliyon.2020.e05808.
- [5] K. Shu, A. Sliva, S. Wang, J. Tang, and H. Liu, 'Fake News Detection on Social Media', *ACM SIGKDD Explor. Newsl.*, 2017, doi: 10.1145/3137597.3137600.
- [6] L. Zheng, Y. Zhang, and V. L. L. Thing, 'A survey on image tampering and its detection in real-world photos', *J. Vis. Commun. Image Represent.*, 2019, doi: 10.1016/j.jvcir.2018.12.022.
- [7] N. Chebib and R. M. Sohail, 'The Reasons social media contributed to 2011 Egyptian Revolution', *Int. J. Bus. Res. Manag.*, 2011.
- [8] N. S. Love, C. Kamath, Q. L. Q. Luo, and T. M. Khoshgoftaar, 'An Empirical Study of Block Matching Techniques for the Detection of Moving Objects Block Matching Techniques', *2007 IEEE Int. Conf. Inf. Reuse Integr.*, 2006.
- [9] J. Ma, X. Jiang, A. Fan, J. Jiang, and J. Yan, 'Image Matching from Handcrafted to Deep Features: A Survey', *Int. J. Comput. Vis.*, 2021, doi: 10.1007/s11263-020-01359-2.
- [10] D. Honzátko and M. Kruliš, 'Accelerating block-matching and 3D filtering method for image denoising on GPUs', *J. Real-Time Image Process.*, 2019, doi: 10.1007/s11554-017-0737-9.
- [11] I. Gede Nengah Bayu Darmawan, G. Made Arya Sasmita, and P. Wira Buana, 'Pengembangan Metode Pendeteksi Modifikasi Citra Menggunakan Metode Error Level Analysis', *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, 2019, doi: 10.24843/jim.2019.v07.i01.p04.
- [12] H. Bisri and M. I. Marzuki, 'Forensik Citra Digital Menggunakan Metode Error Level

- Analysis, Clone Detection dan Exif Untuk Deteksi Keaslian Gambar', *G-Tech J. Teknol. Terap.*, 2023, doi: 10.33379/gtech.v7i2.2363.
- [13] I. Riadi, A. Yudhana, and W. Y. Sulisty, 'Analisis Image Forensics Untuk Mendeteksi Pemalsuan Foto Digital', *Mob. Forensics*, vol. 1, no. 1, p. 13, Sep. 2019, doi: 10.12928/mf.v1i1.703.
- [14] A. Y. Wijaya, S. Al Musayyab, and H. Studiawan, 'PENGEMBANGAN METODE BLOCK MATCHING UNTUK DETEKSI COPY-MOVE PADA PEMALSUAN CITRA', *JUTI J. Ilm. Teknol. Inf.*, vol. 15, no. 1, p. 84, Jan. 2017, doi: 10.12962/j24068535.v15i1.a638.
- [15] S. Ferreira, M. Antunes, and M. E. Correia, 'Exposing manipulated photos and videos in digital forensics analysis', *J. Imaging*, 2021, doi: 10.3390/jimaging7070102.
- [16] R. Maini and S. Mehra, 'A Review on JPEG2000 Image Compression', *Int. J. Comput. Appl.*, 2010, doi: 10.5120/1607-2159.
- [17] Y. Lai, T. Huang, J. Lin, and H. Lu, 'An improved block-based matching algorithm of copy-move forgery detection', *Multimed. Tools Appl.*, 2018, doi: 10.1007/s11042-017-5094-y.
- [18] G. Peterson, 'Forensic Analysis of Digital Image Tampering', in *Advances in Digital Forensics*, Boston: Kluwer Academic Publishers, pp. 259–270. doi: 10.1007/0-387-31163-7_21.
- [19] Nurhidayah, B. Abdul Samad, and B. Abdullah, 'Perbandingan Metode Contrast Enhancement pada Citra CT-Scan Kanker Paru-paru', *Gravitasi*, vol. 19, no. 2, pp. 24–28, Dec. 2020, doi: 10.22487/gravitasi.v19i2.15360.
- [20] H. Lee, J. Lee, H. Kim, B. Cho, and S. Cho, 'Deep-neural-network-based sinogram synthesis for sparse-view CT image reconstruction', *IEEE Trans. Radiat. Plasma Med. Sci.*, 2019, doi: 10.1109/TRPMS.2018.2867611.