IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 3, April 2023
Impact Factor: 7.301

Altered Region Identification in Image Files using Copy-Move Forgery Detection Technique

Y. Sujatha[1], Amit Kumar Mandal[2], Akkireddy Hemanth[3], Appikonda Komali Akanksha[4], Besi Sai Sumanth[5]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5]
Raghu Institute of Technology, Visakhapatnam, AP, India

Abstract: *Nowadays, digital images and videos have high importance because they have become the primary carriers of information. However, the easy availability of powerful image editing software has made it possible to manipulate and edit digital images and videos, leading to a loss of trust in their authenticity. It is possible to add or remove important features from an image without leaving any obvious traces of tampering. To detect this such type of forgeries, the proposed method involves dividing the image into overlapping blocks of the same size, extracting a feature for each block, and representing it as a vector. The vectors are then sorted using radix sort, and the difference in the positions of adjacent feature vectors in the sorted list is computed to obtain a shift vector. This method can even identify tampered parts of an image that have been enhanced or retouched to merge with the background or saved in a lossy format like JPEG. Several forged images were tested to demonstrate the effectiveness of this proposed method. Its application has significant implications in fields like forensics, journalism, and medical imaging to ensure the authenticity of digital images and videos.*

Keywords: Altered Region Identification, Copy-Move Forgery Detection Techniques, Shift Vector, Radix, Double JPEG Compression ,Grey scale.

I. INTRODUCTION

The prevalence of various social media platforms encourage individuals to manipulate photographs to enhance their quality and appearance, often for deceptive purpose [1]. Various methods of digital image manipulation are utilized in the context of forgery, with the intention of gaining fraudulent advantages or creating misleading perceptions[2]. Nowadays digital images should not be trusted and must be verified before being accepted as accurate representations of reality[3]. As stated earlier, manipulated images have a harmful effect on viewers and can lead to misunderstandings of people and events. There are two types of methodologies that can be used to detect digital image forgery : active and passive methods analyse the image for irregularities or inconsistencies that suggest tampering[4]. Copy-Move is a type of image manipulation where a portion of an image is copied and pasted into another section of the same image. In this method , the image is overlaid with a circularly shifted version, and the closely matching image blocks are searched for. This method is efficient and effective for small-sized images[5]. However, for medium-sized images, it can be computationally expensive and even impractical since each shift requires multiple autocorrelation, which identifies the correlation complexity and often fails to detect forgeries[6].

II. EXISTING SYSTEM

There are two types of studies on passive-based forgery image detection currently available. The one employs DCT coefficient analysis to detect the splicing forgery image, while the other depends on recognizing the copy-move forgery image. The next sections go through two well- known strategies.

2.1 Double JPEG Compression

The process of double JPEG compression involves compressing an image with two different quantization matrices: the initial matrix q1 and the secondary matrix q2. If q1 and q2 are not equal, the DCT coefficients are considered to be

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 3, April 2023
Impact Factor: 7.301

doubly compressed. Lin et al proposed a method for detecting tampered JPEG images using DCT coefficient analysis, specifically by analysing the compression levels of the image . image containing a double quantization (DQ) effect is necessarily a forgery was found to be incorrect[7]. Mainly focused on JPEG images and proposed a method for detecting tampered images by analysing the DQ effect that is present among the DCT coefficients. Their approach involved identifying subtle differences between the DCT coefficients of the original and tampered images, which can be indicative of tampering[7].

2.2 Speeded Up Robust Features (SURF)

This algorithm has been chosen for its excellent computational characteristics for our specific application. The SURF algorithm consists of three main steps. The first step involves creating SURF keypoints, which are specific points in the image that are relevant for feature detection[8]. Next, interest spots in the image are identified, and a local feature description is generated for each interest point. Finally, these local features are used for matching and comparing images. Overall, the SURF algorithm is an effective method for identifying key features in images and is widely used in computer vision and image processing application.

III. RELATED WORK

The proposed forgery detection technique comprises two primary stages: splicing and copy-move forgery detection. The block diagram of the proposed algorithm is shown in Figure 1. The algorithm is designed to detect forgeries in JPEG compressed images. If the original image is in another lossless format, it is first converted to JPEG format with the highest compression quality. Next, the image is converted to the YCbCrcolor space. To initialize the block processing parameters, the block size is set to Mb=8 and the search range of the neighbourhood is (Iwidth/Mb) × (Iheight/Mb). After pre-processing, the algorithm proceeds to detect splicing and copy-move image forgeries, as described in the following sections[9].

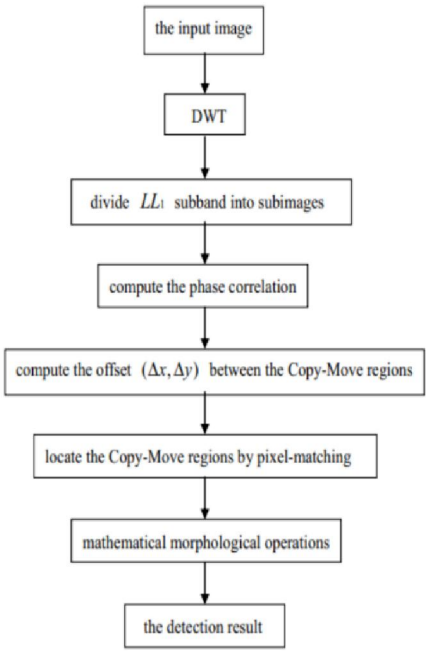


Fig 1:Block diagram of proposed methodology

The Fourier Mellin Transform (FMT) has recently been proposed as a method for image block analysis. This technique involves obtaining the Fourier transform representation of each block and then re-sampling the resulting magnitude values into log-polar coordinates. From there, a vector representation is obtained by projecting the log-polar values onto a 1-D axis, which is used as a feature for detection. The authors of this paper have shown that their technique is robust to compression up to JPEG quality level 20, as well as rotation up to 10 degrees and scaling up to 10%. Another method proposed by Hwei-Jen Lin et, involves extracting a 9-dimensional feature vector for each block of size

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 3, April 2023
Impact Factor: 7.301

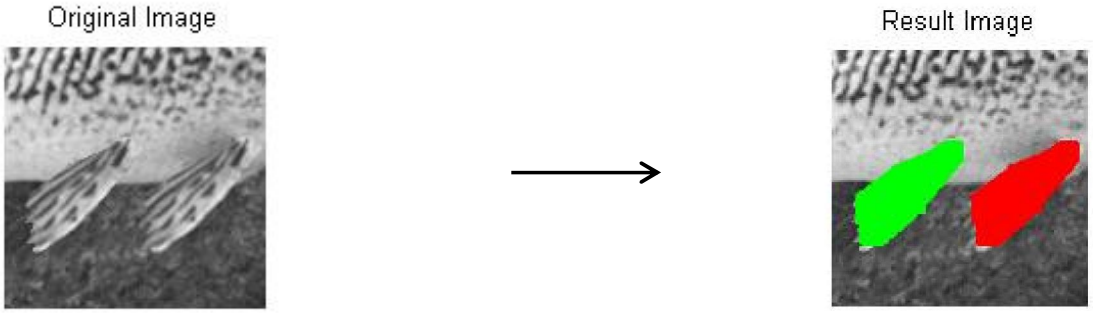
16x16[10].Unlike other techniques that store the feature vectors as floating numbers, this method stores them as integer values, which are sorted using the radix sort algorithm for more efficient detection without degradation of detection quality. The difference, or shift vector, of the positions of every pair of adjacent feature vectors in the sorting list is then computed[11].

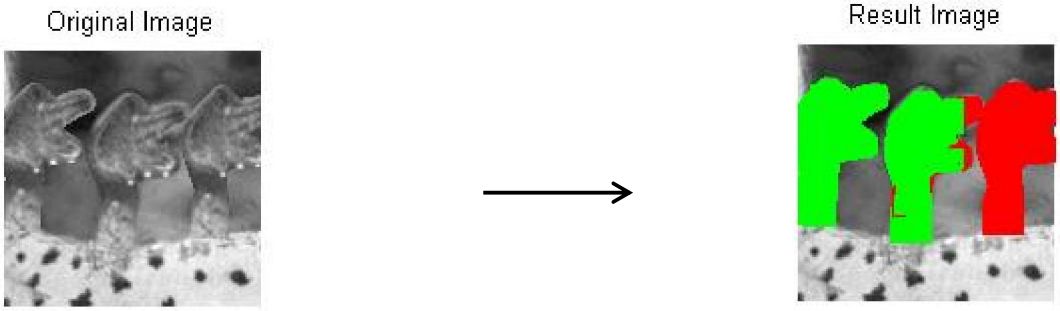
IV. METHODOLOGY

This technique uses a feature vector representation of image blocks, which are sorted using radix sort to reduce the detection time complexity. The method then evaluates the accumulated number of each shift vector, identifying large accumulations as possible duplicated regions. The corresponding feature vectors are then marked to form a tentative detected result, which is further processed using connected component analysis and medium filtering to obtain the final result. However, the method may not be able to detect all copied regions of smaller size[12]. The authors also noted that the technique performed well with rotations of 90, 180, and 270 degrees, suggesting that it may not be as effective for other degrees of rotation. The duplicated regions may form identical shift vectors or different shift vectors that are rotated through a certain degree.

In copy-move forgery, the tampered region still shares most of its inherent characteristics, such as the color palette or pattern noise, with the remainder of the image. Therefore, a structural analysis of image regions might reveal a high level of similarity between the duplicated regions[13]. The proposed algorithm in the passage uses DWT, FFT, and mathematical morphological operations to detect copy-move forgery in an image.The proposed technique can detect both copy-move and splicing image forgery. If the final outcome is a non-forged image, it means that the image is authentic and no tampering has been detected. If the final outcome is a splicing image, it means that the image has been tampered with using the splicing technique[14]. If the final outcome is a copy-move image, it means that the image has been tampered with using the copy-move technique. The technique also considers the possibility of JPEG compression in the suspicious image and suggests that it can still be recognized using the splicing approach[14].

V. RESULTS





IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 3, April 2023
Impact Factor: 7.301

VI. CONCLUSION

The proposed algorithm is designed to detect Copy-Move forgery in digital images automatically and effectively by using the idea of pixel-matching. The algorithm has a lower computing complexity and is resistant to various types of Copy-Move post-processing. The results of the experiments show that the proposed technique is effective in detecting forged regions and locating non-original regions. The proposed technique uses SURF descriptors' feature keypoints to locate duplicates of the same object and double JPEG compression analysis of DCT coefficients. Compared to previous methods, this algorithm has a lower computing complexity and is more resistant to various types of post-processing. Experimental results demonstrate that the proposed technique is successful in detecting forged regions and locating non-original regions. The algorithm utilizes two approaches, namely, feature keypoints of SURF descriptors to locate duplicates of the same object and double JPEG compression analysis of DCT coefficients to detect copied and pasted image portions. The proposed technique can also detect multiple items. Although sophisticated tools and advanced manipulation techniques have made forgery detection more challenging, the field of digital image forensics is still in its infancy, and there is still much work to be done. The authors plan to continue their research by detecting other types of digital forgery, such as spliced images, photorealistic computer graphics, and video forgery.

VII. FUTURE SCOPE

We use radix sort to improve time complexity and adopt features that can resist various attacks such as JPEG compression and Gaussian noise. Our experimental results demonstrate high detection rates and efficiency, but we were unable to successfully detect a few small copied regions. Our method can detect duplicated regions with rotation through fixed angles, but it does not handle rotation at arbitrary angles. In the future, we plan to search for feature invariants that can handle this problem. We also aim to extend our work to video images. With the growing popularity of passive picture authentication solutions, several new algorithms have been presented to address image authenticity. As copy-move forgery is the most common type of forgery, we focused our research on algorithms dedicated to it. To facilitate comparison, we selected one algorithm from each category to represent it.

REFERENCES

[1]. Sri, C.G., Bano, S., Trinadh, V.B., Valluri, V.V. and Thumati, H., 2022. Detection of Image Forgery for Forensic Analytics. In Sustainable Advanced Computing (pp. 321- 338). Springer, Singapore

[2]. Bohari, B. and Rahim, N., 2021. A comparison between Speeded Up Robust Features (SURF) and Discrete Wavelet Transform (DWT) as feature extraction in Copy-Move Forgery Detection. Applied Information Technology And Computer Science, 2(2), pp.21-36.

[3]. Abbas, M.N., Ansari, M.S., Asghar, M.N., Kanwal, N., O'Neill, T. and Lee, B., 2021, January. Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks. In 2021 IEEE 19th World Symposium on Applied Machine Intelligence and Informatics (SAMI) (pp. 000125-000130). IEEE.

[4]. Raskar, P.S. and Shah, S.K., 2019, September. A Fast Copy-Move Forgery Detection Using Global and Local Features. In 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-4). IEEE.

[5]. Gupta, A., Kumar, A., Chaudhary, T. and Leekha, A., 2021, August. Detection and Localization of Tampered Image using Hash Functions. In 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 198-203). IEEE.

[6]. Hebbar, N.K. and Kunte, A.S., 2021, December. Image Forgery Localization Using U-Net based Architecture and Error Level Analysis. In 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1992-1996). IEEE.

[7]. Rajkumar, R., Roy, S. and Manglem Singh, K., 2019. A robust and forensic transform for copy move digital image forgery detection based on dense depth block matching. The Imaging Science Journal, 67(6), pp.343-357.

[8]. Rakesh, S. and Sanjay, S., 2018. Ameliorating the Performance of a Hybrid CMFD Technique. International Journal of Applied Engineering Research, 13(22), pp.15511-15518.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 3, April 2023
Impact Factor: 7.301

[9]. J.A. Redi, W. Taktak, J.L. Dugelay, Digital image forensics: a booklet for beginners, Multimedia Tools Appl. 51 (1) (2011) 133–162.

[10]. T.-T. Ng, S.-F. Chang, A model for image splicing, in: International Conference on Image Processing (ICIP 04), vol. 2, 2004, 1169–1172.

[11]. Sharma, V. and Singh, N., 2021, November. Deep Convolutional Neural Network with ResNet-50 Learning algorithm for Copy-Move Forgery Detection. In 2021 7th International Conference on Signal Processing and Communication (ICSC) (pp. 146-150). IEEE

[12]. Sunkara, S.C., Balaji, R. and Babu, M., 2020. A critical investigation on ultrasound cyber-attack and using fourier transform for defence application against inaudibleattacks. Materials Today: Proceedings

[13]. Singh, B. and Sharma, D.K., 2021. SiteForge: Detecting and localizing forged images on microblogging platforms using deep convolutional neural network. Computers & Industrial Engineering, 162, p.107733.

[14]. Majumdar, P., Agarwal, A., Singh, R. and Vatsa, M., 2019. Evading face recognition via partial tampering of faces. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops