International Journal of Scientific Research & Engineering Trends
Volume 9, Issue 3, May-June-2023, ISSN (Online): 2395-566X

Video Forgery Detection Using Machine Learning

Ankita Malage, Vidya Kesarakar, Bhavana Sarapure, Asma Nadaf, Prof. Neelamma Shinannavar

Department of Computer Science & Engineering.
VSMSRKIT Engineering College. Nipani
ankitamalage9424@gmail.com, vidyakesarkar2501@gmail.com, bhavanajagadeesh6@gmail.com, amnadaf410@gmail.com, shinannavarneelamma1997@gmail.com

Abstract- Region duplication is a very easy and effective method to create digital image forgeries, where a continuous portion of pixels in an image are copied and pasted to a different location in the same image. Nowadays Video and image copy- move forgery detection is one of the major hot topics in multimedia forensics to protect digital videos and images from malicious use. The Number of techniques has been presented through analyzing the side effect caused by the copy-move operation. In this paper, we propose a novel approach to detect copy-move forgery. And also coarse-to-fine detection strategy based on optical flow (OF) and stable parameters is designed to detect. The detected image is initially divided into overlapping blocks. After the creation of overlapped blocks, the feature extraction technique is applied to the image to extract the features from specific blocks of the image to identify duplicate blocks of an image.

Keywords- Machine learning, Video forgery detection using machine learning.

I. INTRODUCTION

There is a significant role of digital images and videos in our daily life. Video is nothing but the collection of images or frames. However, image tampering has become very easy by using powerful software. Videos or images can be scanned using the software and tampered with without any doubt. Now a day image authenticity is a big concern. Image forgeries may have many types- such as copy-move forgery, splicing, and many more. Copy-move forgery is nothing content of another image and pasting it into the same image which we want to forge. The two main types of image forensic techniques are to verify the integrity and authenticity of manipulated images. One is an active forensic method and another is a passive forensic method. In active methods watermarking and steganography are two techniques that are used to insert authentic information into the image. In the authenticity of an image, the prior embedded authenticity information is recalled to prove the authenticity of that image. However, embedding the authentication of information to an image is very reliable. Only authenticated users are allowed to do it or at the time of creating the image, authentic information could be embedded as well. But the requirement of special cameras and multiple steps processing of the digital image are two main limitations that made this technique less efficient. To avoid these limitations, passive forensic techniques utilize image forgery without requiring detailed previous Information. The most widely used method to make forged image copies is a copy- move forgery. It refers to copying one part from another image and pasting it inside the same image. Sometime before pasting the copied regions, blurring, intensifying or JPEG compression may be applied.

II. LITERATURE SURVEY

A. Block-Based Image Forgery Detection The In block-based method, the input image size of M x N is segmented into overlapping blocks size of z x z resulting into overlapping blocks, L = (M- z+1) x (N-z+1). A few features are extricated from each block. Distinctive features are extracted by applying different feature extraction techniques such as DCT (Discrete Cosine Transform) [9], DWT (Discrete Wavelet Transform) [10], DFT (Discrete Fourier Transform) [10], PCA (Principal Component Analysis) [12] [13], SVD (Singular Value Decomposition) [14][15], and ZMs (Zernike Moments) [16]. Then, a comparison is done based on the block's features similarity and distance. After finding the most matched or similar features of the block, the copy-move region is identified and this region is localized. Sheng et al. [9] proposed a forgery detection algorithm using a block-based method. This uses DCT and circle-blocking techniques for extracting features of the image. Finally, the image which contains singularities within lines is presented by computing ridgelet transformation. Robustness against JPEG compression is the most significant feature of this method. Cao et al. [17] followed a block-based method to detect tampered regions where the DCT feature extraction technique is applied. DCT is used to divide subblocks to extract key features by producing quantized coefficients.

B. Key Point-Based Forgery Detection Method It is different from block-based methods, features are extracted

in key point-based methods from the image without any type of segmentation. Extracted features from every key point are compared to find similarities between them. Finally, based on the calculation of matched features, image forgery is detected. SIFT and SURF (Speeded Up Robust Features) are two main key points-based feature extraction methods. Somayeh Sadeghi et al. [21] and Diaa M. Uliyan et al. [22] worked on key point-based techniques (e.g. SIFT). Sadeghi et al. proposed SIFT to extract features and search for similar features based on their Euclidean distance. Both methods are robust against several post- processing attacks; including scale, noise, rotation, and JPEG compression. However, the inability to detect small forged areas and the performance of detection and localization for those forged areas are also questionable. In [22], the primary approach of Uliyan et al. was to detect image regions by using Statistical Region Merging (SRM) Segmentation algorithm. Then, the experiment proceeded with applying Angular Radial Partitioning (ARP) and Harris Corner detection methods on the image region. Finally, forged regions were detected based on matched key points. The method showed less robustness against forged regions with blurring and illumination attacks. Moreover, it shows different results for the same image with different resolution. The major drawbacks of the previously mentioned conventional techniques are either not powerful against all post-processing attacks or high computation time. Therefore, keeping up the low computational time is the most important robustness challenge. To tackle this issue, a new copy-move forgery detection method is proposed where region-wise image segmentation is done. Gabor filters are used to extract image features. Afterward, K Means clustering and Euclidean distance calculation facilitated to detection of forged regions from the suspicious image. Reducing the false matching rate is the most significant task to exhibit the proposed method as more video compared to video conventional methods.

C. Video Input Video forensics has become an important area of research in the last decade. The System will accept video as input. The Justified format of the video should be given as input to get processed.

D. Video Parsing / Segmentation The Input video is been accepted and done parsing based on fps. These frames will be temporarily stored in the backend for further processing and feature extraction.

E. K-Means Clustering K-means clustering is a technique for quantizing vectors. This method divides the image into k segments, each containing mutually exclave data. This is a common method when it comes to pattern recognition and machine learning. One of the segmented images is chosen based on the based on of the information contained in it. To determine this, the features of each segment are calculated and the segment with the highest mean is chosen. The features of the segmented image are then compared with the original image using cross- validation, which gives another array, which is studied to determine whether an image is morphed or not, and the function for the final result is added based on that.

F. Feature Extraction Out of all the methods to analyze an image, extraction of GLCM features has proven to be efficient time and time again. The gray-level co- variance matrix is a tabulation that provides statistical measures for texture analysis. This method takes into account the spatial relationship between the intensities of pixels in a gray-level image. In this paper, the GLCM features were calculated to study the differences between the original image and the digitally forged image. This gave 22 texture values (for each image) to work with, most of which were similar when it came to an image and its fraudulent counterpart. In practice, this would lead to redundancy and would also increase the time to run the algorithm. Also, the histogram of oriented gradient (HOG) features was calculated which gave another set of features for the original and the morphed image. The HOG values of the original and the morphed images were reasonably apart from each other, which meant that these values will be useful in differentiating the original document from the morphed one. However, the order of the matrix generated by the HOG algorithm is too large to be successfully fed into an SVM so it could also not be of practical use.

G. Online Database The Feature values were computed but since the order of the matrix produced was very large it was trained by using the ANN machine learning algorithm to enhance accuracy.

H. Detection Of the Forged Region After the identification of duplicate blocks, the further step is to highlight the duplicate blocks on the digital image, which also indication of forged regions. Hence, the system finally detects forged areas in the digital image. The corresponding forged regions are highlighted by the system.

III. SYSTEM OVERVIEW

A. Creation Of Non-Overlapped Blocks In this approach, the detected image is initially divided into overlapping blocks. The basic approach here is to detect connected blocks that have been copied and moved. The copied area consists of many overlapping blocks. The further step would be extracting features from these blocks.

B. Feature Extraction Technique After the creation of the overlapped blocks, the feature extraction technique is applied to the image to extract the features from specific blocks of the image. In this work approximation image, the local binary pattern features method is applied to the block region for extracting the features. AILBP (Approximation image Local Binary Pattern) Initially on the face images, a bi-level wavelet decomposition method

has been applied, which has transformed face images into approximation images. Then, on approximation images, local binary patterns (LBP), have been used to extract local features of the face images. The AILBP method is a combination of wavelets decomposition along with the LBP method which is effective in terms of accuracy and it reduces time computation.

C. Wavelet decomposition The Wavelet breakdown method is an occurrence of time and signal analysis method. It can be applied to decompose a forged image into many sub-band images with variations in spatial resolution, characteristics of frequency, and directional features [10]. In this method, the approximation and details coefficients are computed by decomposing the face image up to two levels. Approximation coefficients pick the lowest frequency components and details coefficients contain the highest frequency component of an image. Only approximation coefficients are taken for further procedure. Approximation coefficients contain low-frequency components of the forged image, which contain the whole information of the image. The variation of expression and small scale obstruct do not alter the low-frequency part but the high-frequency portion of the image only. More than two steps of decomposition of forged image result in information loss and hence, not involved in this work.

D. Identification of the duplicate Rows in a feature matrix In the feature matrix, each row represents a specific block. To detect the duplicate rows, first, from the feature matrix, the system finds out the number of rows in which the original feature matrix is being compared with filtered-out resultant rows which are duplicates. Hence, such a comparison gives blocks that are duplicated in the feature matrix.

IV. PLANING

1. Define project objectives.
2. Break the project into a list of deliverables and milestones.
3. Define tasks for each deliverable and milestone.
4. Estimate the time and resources needed for completion.
5. Identify risks.
6. Identifying results and obtaining their input.
7. Identify requirements
8. Evaluate the results and take action to complete any outstanding requirements.

V. ARCHITECTURE DESIGN

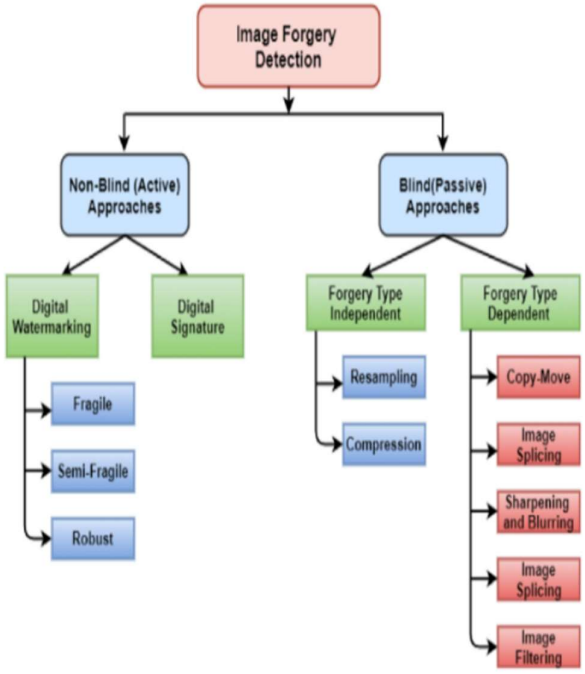

Figure 1 – Dfd.

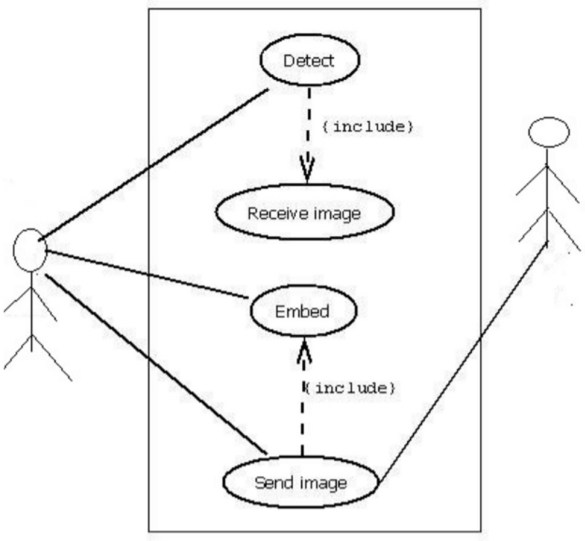

Figure 2 – Use Case.

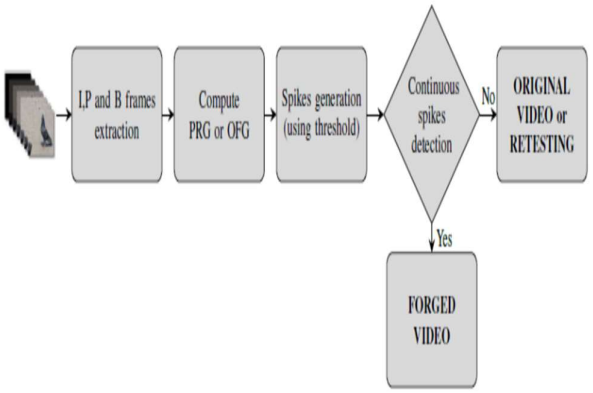

Figure 3 – Sequence Diagram.

V. METHODOLOGY

- Video Forgery Detection aims to establish the authenticity of a video and to expose the potential modifications and forgeries that the video might have undergone.
- Undesired post-processing operations or forgeries generally are irreversible and leave some digital footprints.
- Video forgery detection techniques scrutinize these footprints to differentiate between the original and the forged videos.
- When a video is forged some of its fundamental properties change and to detect these changes is what is called Video Forgery Detection techniques used.

VI. ADVATAGE AND APPLICATION

1. Efficient
2. Less Time Consuming
3. Low-level tempering
4. Capturing frame by frame Tampering
5. Mass level Tampering
6. Voxel-level Tampering.

VII. CONCLUSION

Among the fastest-growing area of research in the field of video forgery detection is passive- blind methods and detection methods to verify the integrity and authenticity of digital video sequences. To this end, current studies dedicated to passive- blind methods do not need prior knowledge of the video frames content or pre-embedded watermarks or signature. In this study, the issue of digital video manipulation detection is discussed with references to blind methods of video forgery detection. Various frames of video forgery detection methods are categorized and generalized in this paper and the rendering of some typical video forgery detection algorithms methods are compared. Some of the developed approaches for the detection and determination of video manipulation is capable of localizing tampered object locations of frames sequence. This study's findings are expected to contribute to methods and ideas in the field of digital video forgery detection.

REFERENCES

[1] Shruti Ranjan, Prayati Garhwal, Anupama Bhan, Monika Arora, Anu Mehra " Framework For Image Forgery Detection And Classification Using Machine Learning", IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN:978-1-5386- 2842-3.
[2] H M Shahriar Parvez, Hamid A. Jalab, and Somayeh Sadegh, "Copy-move Image Forgery Detection Based on Gabor Descriptors and K- Means Clustering (ICSCEE2018) ©2018 IEEE. [3] R. Poisel and S. Tjoa, "Forensics investigations of multimedia data: A review of the state-of-the-art," in Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011, 2011, pp. 48–61.
[4] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no. 3, pp. 226–245, 2013.
[5] G. Lynch, F. Y. Shih, and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," Inf. Sci. (Ny)., vol. 239, pp. 253–265, 2013. [6] H. C. Hsu and M. S. Wang, "Detection of copy- move forgery image using Gabor descriptor," in Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID, 2012.
[7] D. M. Uliyan, H. A. Jalab, A. Abuarqoub, and M. Abu-Hashem, "Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor," in Proceedings of the International Conference on Future Networks and Distributed Systems, 2017, p. 6:1--6:6.
[8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.
[9] G. Sheng, T. Gao, Y. Cao, L. Gao, and L. Fan, "Robust algorithm for detection of copy-move forgery in digital images based on ridgelet transform," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012, vol. 7530 LNAI, pp. 317–323.