SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 /doi:10.14445/23488387/IJCSE-V8I8P102
Volume 8 Issue 8, 8-12, Aug 2021

Image Forgery Analyse and Detection

Alhussain Akoum [1], Samia Bahlak [2], Nagham Abou Daher[3]

[1]*Faculty of Technology,CCNE Department, Lebanese University, Mujamaa Bahaa Street Saida, 1600, Lebanon.*
[3]*A Student from Faculty of Technology, GST Master, Lebanese University, Lebanon*

Received Date: 05 July 2021
Revised Date: 08 August 2021
Accepted Date: 20 August 2021

Abstract *- The popularity of digital photography has risen in recent years, paving the opportunity for new and inventive ways to create photos. Several software programs are now available that may be used to edit images such that they like the original. In the case of any crime, images are used as authenticated proof, and if they do not remain real, it will pose a problem. In recent years, detecting these types of forgeries has become a big difficulty. It's difficult to tell whether a digital image is real or doctored. Finding tampering marks in a digital image is a difficult undertaking. A copy-move image forgery is used to hide an image object or to add more details to the image, resulting in forgery. In both circumstances, image reliability is jeopardized. Although this technology has numerous benefits; it can also be used as a deceptive technique to hide facts and evidences. In this article, we looked at many types of picture forgery and detection strategies; we concentrated mostly on copy move forgery and its detection technique.*

Keywords — *Image forgery, Copy move, Detection Technique, Digital image, Tempering marks*

I. INTRODUCTION

Image tampering isn't a new concept; It can be traced back to the invention of photography.. However, with the invention of easily available digital cameras and picture manipulation software tools, it is now in the spotlight. The earliest known fake image was of Hippolyta Bayard, who in 1840 issued a fake photograph of himself committing suicide as an act of nuisance in order to avoid losing the title of inventor of photography to Louis Daguerre in 1840 [1]. Because of the development of easy-to-use and low-cost tools, digital visual media has become one of the most popular methods of conveying information. Furthermore, visual media has more expressive possibilities than any other medium. It explains sophisticated scenes in a straightforward manner, which can be difficult to copy in other ways. Digital Image Forgery is the intentional alteration of digital images with the purpose to deceive in order to change public perception. The modification is done out in such a way that no apparent traces remain. With the introduction and widespread availability of useful picture editing tools and software, digital image manipulation is no longer limited to specialists. Sumopaint, Paintshop Pro, Photoshop CC, and HitFilm Express are some of the most well-known image editing programs available online [2]. As a result, the validity of an image must be verified. This type of verification is carried out using image forgery detection techniques. These methods are used to check the authenticity of images. There are many styles of image forgery exposed thus far and correspondingly the forgery detection techniques. There are two approaches for detecting image manipulation in digital images. The first is an active-based method, whereas the second is a passive-based one. Digital watermarks and signatures are two types of active based approaches. For the detection of tampered regions in photographs, digital watermarking and signature methods have been employed in the past, but these approaches need preprocessing of the data, which makes them difficult to deploy[3]. Another alternative is to take a more passive approach. We don't need any image information to use this method. In this method, we extract various intrinsic features traces from the digital photo image in order to discover suspicious locations. To detect the tampered region, we use the fake image as an input. As a result, a passive strategy is preferred.

Furthermore, an active-based technique necessitates additional procedures and degrades the original image, so a passive-based approach is preferable to an active-based approach. Many scholars have been devoted to the topic of picture forensics since the introduction of synthetic images, aiming at various image forgeries methods such as copy-move, splicing, retouching, filtering, and double JPEG (joint photographic experts group) compression.

The remainder of the paper is laid out as follow: image tempering techniques, forgery detection technique, and related work regarding copy-move forgery detection (CMFD), the details of proposed algorithm, experimental results and finally the conclusion.

II. IMAGE TEMPERING TECHNIQUES

The image can be forged by adding, removing, or changing specific portions in the original image, with the sole requirement being that no physically visible evidence is left behind. To create a picture, several ways can be utilized; these methods are typically classified as indicated in **Fig 1.**

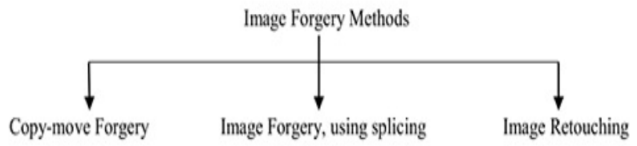

Fig 1: Types of image forgery.

A. Copy Move Forgery: As seen in **Fig 2.** Copy-move forgery entails duplicating a portion of a photograph and pasting it into another section of the same image. The idea is to hide some of the original image's details. It's one of the most common methods of creating an image. There are no evident substantial alterations because the duplicated part is of the same image. As a result, recognizing it is frequently challenging.

(a) original image (b) forgery image

Fig 2: Effect of Copy Move forgery.

B. Image Splicing: It's a grouping of one or more photos. The images are blended to form a new image. It makes uses of cut/copy/paste procedures. A portion of one image is cut out and put into another. To completely merge the cut/copied section of an image into another image, several post-processing steps are required, as shown in **Fig 3.** The image's pattern is disrupted by the pasted piece. As a result, image pattern analysis aids in the detection of image forgeries.

Fig 3: Image splicing by using two different images.

C. Image Retouching: As shown in **Fig 4.** The image does not changed fundamentally, but there is an augmentation and decrease of a certain characteristic of the original image. It's a damaging picture fabrication that's gentle. It's a technique employed by magazine photo editors to make photographs more appealing. It's possible that such improvement is wrong.

Fig 4: Before and after retouching image.

III. FORGERY DETECTION TECHNIQUE

The active method and the passive method are two types of digital picture forgery detection approaches. In the active technique, a digital watermark is placed inside an image during its development to embed certain information. The disadvantage of this strategy is that a watermark must be added during the recording process, which would limit the use of specially equipped digital cameras. In the passive technique, during the generation of an image, there is no pre-embedded information. This method solely relies on analyzing an image's binary content. Techniques for detecting picture forgeries that are passive are divided into five groups [4].

A. Pixel-Based Image Forgery Detection: Pixel-based approaches emphasize on the digital image's pixels. Copy-move, splicing, retouching approaches are the three types of techniques used. Among the well-known phony identification techniques, this is the most prevalent image manipulating technique.

B. Format-Based Image Forgery Detection: Another type of picture forgery detection approach is format-based techniques. These are primarily based on image formats, with JPEG being the preferred format. Image forgery detection is aided by statistical correlation introduced by specialized lossless algorithms. JPEG quantization, Double JPEG, and JPEG blocking are three different types of JPEG approaches. It is extremely difficult to detect fraud in compressed images, yet these techniques can detect forgery in compressed images.

C. Camera-Based Image Forgery Detection: When we take a photo with a digital camera, the image passes through a series of processing stages, including quantization, colour correlation, gamma correction, white balancing, filtering, and JPEG compression, as it flows from the camera sensor to the memory. These processing steps, from image capture to image storage in memory, may vary depending on camera model and camera age. This standard serves as the foundation for these procedures. Chromatic aberration, colour filter array, camera response, and sensor noise are the four types of approaches that can be used.

D. Physical Environment-Based Image Forgery Detection: These methods rely on three-dimensional interactions between the physical object, light, and the camera. Consider creating a fake depicting two movie stars who are supposed to be romantically connected walking down a night-time shoreline. Individual photographs of each movie star may be grafted together to create such a picture. Lighting contrasts can be used to demonstrate that an image has been manipulated. These methods are based on the lighting situation in which an article or photograph is captured. Lighting is vital when it comes to photographing something. Light direction (2-D), light direction (3-D), and light environment are the three classifications for these techniques.

E. Geometry-Based Image Forgery Detection: The fundamental element of these techniques is the projection of the camera center into the image plane, which allows for the measurement of objects in the actual world and their position in relation to the camera. Grooves in handgun barrels give the shot a twist, which improves accuracy and range. These grooves acquaint the bullet shot with certain markings to some extent, and can thus be used with a specific firearm. Several image forensic approaches that specifically display relics presented by distinct steps of the imaging procedure have been developed in the same spirit.

IV. RELATED WORK

For detecting copy move forgery, a variety of approaches have been proposed by various authors.

In [5,] Fridrich et al. demonstrated for the first time the copy-move forgery detection technique using DCT on tiny overlapping blocks. The feature vectors are created using DCT coefficients. After lexicographically sorting the feature vectors, the similarity between blocks is examined.

In [6,] picture blocks are represented using principal component analysis (PCA).The authors used nearly half of the amount of features used by [5] by utilizing one of PCA's features. It improves the effectiveness of this technique, but it fails to identify copy-move forgery when rotated.

[7] Proposes a sorted neighborhood algorithm based on the Discreet Wavelet Transform (DWT). The image is divided into four sub bands to create the feature vector, and the Singular Value Decomposition (SVD) is used on the low frequency components. The method is only resistant to JPEG compression up to quality level 70.

[8] Introduces a technique for extracting block features and Kd-Treematching based on blur moment invariants up to seventh order.

[9] Proposes a method for identifying image forgeries based on DCT and SVD. The technique has been found to be resistant to compression, noise, and blurring, but it fails when images are rotated even slightly.

[10] Proposes a direct block comparison-based efficient expanding block approach.

The authors of [11] used the polar harmonic transform (PHT) to extract feature vectors from circular blocks in order to detect image forgery.

V. OUR EXPERIENCE

In proposed methodology, copy-move forgery is detected by dividing the image into overlapping blocks, and then extracts the feature from each block by using SVD (different feature extraction methods can be used like PCA, DCT, and DWT), sort these features in lexicographic order and finally locate similar blocks. The proposed method enhances performance by reducing detection time and robust to many post-processing techniques. Figure 5 depicts a flowchart for detecting copy-move forgeries. This describes the entire process of detecting copied regions from a forged image.

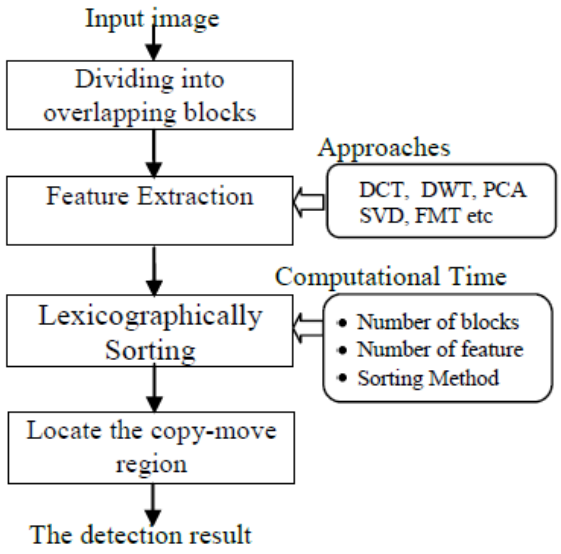

Fig 5: Block diagram of copy move forgery detection.

A. choose the forged image as the input.

B. Applying the "iminfo "function in order to have some information about the forged image before starting detection.

C. Dividing the gray scale image into overlapping blocks of size "b", b is the number of pixels per block.

D. Feature extraction using singular value decomposition SVD using $A=USV^T$ where S is the non-zero singular values of A are the square roots of the non-zero eigenvalues of both V and U.

E. Make an N_b*b matrix with the singular values as the rows, N_b is the total number of blocks.

F. Sort the rows of the above matrix in lexicographic order to create matrix S. Let Si denote the rows of S and (xi, yi) denote the position of the image coordinates of the block that corresponds to Si.

G. Locate similar blocks:

a) For every pair of rows S_i and S_j from S such that $|i - j| < Nn$ (Nn number of neighboring

rows to search in the lexicographically sorted matrix), place the pair of coordinates (x_i, y_i) and (x_j, y_j) onto a list.

b) Compute the offsets of all the elements in this list, which are defined as:
$(x_i - x_j , y_i - y_j)$ if $x_i - x_j > 0$
$(x_j - x_i , y_i - y_j)$ if $x_i - x_j < 0$
$(0, |y_i - y_j|)$ if $x_i = xj$

c) Discard all pairs of coordinates with an offset frequency less than Nf (Nf is the minimum frequency threshold).

d) Discard all pairs whose offset magnitude, $\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$, is less than Nd (Nd is the minimum offset threshold).

e) Create a duplication map using the remaining pairs of blocks by creating a zero picture of the same size as the original and colouring all pixels in the duplicated region with a unique gray scale intensity value.

f) If no similar blocks a message appears on the screen that is no copying detected.

VI. EXPERIMENTAL RESULTS

This section presents the experimental results of the proposed technique.

The performance of the proposed technique is evaluated on dataset collected from the Internet containing the images of sizes 224×224 and 257×180 pixels.

MATLAB is used to test the images where we set the parameter values for "b" =8, Nn=10, Nf=129, Nd=50;

Fig 6: Input image **Result**

Fig 7: Input image **Result**

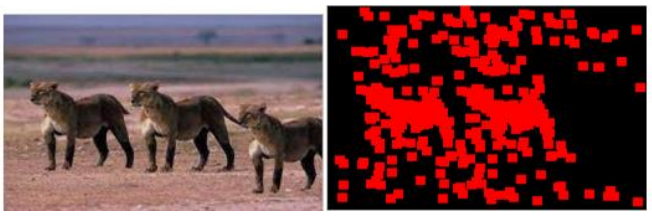

Fig 8: Input image **Result**

VII.CONCLUSION

A novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching is proposed in this project. The propose scheme integrates both block-based and key point-based forgery detection methods. First, the propose Adaptive Over-Segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Experiments show that the suggested technique performs well under a variety of difficult situations, including geometric transforms and JPEG compression. Future research could work on adapting the suggested adaptive over segmentation method to other types of forgery, such as splicing, or to different types of media, such as video and audio. Another avenue for future research is to combine the forgery detection method with several watermarking methods [12-13] to increase multimedia security.

ACKNOWLEDGMENT

A Project is innovative paintings of many minds. A Proper synchronization between individual is a must for any project to be finished successfully.

Though words aren't sufficient to explicit my gratitude to all the ones who've contributed in making this project, I am thankful to Dr. Hussain Al Akoum and Dr.Samia Bahlak, my project mentor, for their valuable advice, criticism and positive appreciation .

I am thankful to get constant encouragement, support and guidance from my parents. Moreover I would like to thanks my husband for giving me strength and patience to work. Finally, I would love to explicit my way to all those, who've helped me immediately and indirectly.

REFERENCES

[1] M. Ali and M. Deriche, Signal Processing Image Communication, 39 (2015) 46–74.

[2] J. Fridrich, D. Soukal and J. Luk´a˘s, Detection of Copy-Move Forgery in Digital Images, International Journal, 3 (2003) 652–663.

[3] S.Khan, A. Kulkarni, An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform, IJCSE, 2(5) (2010) 1801-1806.

[4] Farid, A survey of image forgery detection, IEEE Signal Process.Mag. 26(2) (2009) 16-25.

[5] J. Fridrich, D. Soukal, and J. Luk´a˘s, Detection of copy-move forgery in digital images, in Proceedings of Digital Forensic ResearchWorkshop, Cleveland, Ohio, USA, August 2003.

[6] Popescu and H. Farid, Exposing digital forgeries by detecting duplicated image regions, Tech. Rep. TR2004-515, Dartmouth College, Hanover, NH, USA, 2004.

[7] Li, Q. Wu, D. Tu, and S. Sun, A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD, in Proceedings of IEEE International Conference on Multimedia and Expo (ICME '07), (2007) 1750–1753, IEEE, Beijing, China.

[8] B.Mahdian and S. Saic, Detection of copy-move forgery using a method based on blur moment invariants, Forensic Science International, 171(2-3) (2007) 180–189.

[9] [9] J. Zhao and J. Guo, Passive forensics for copy-move image forgery using a method based on DCT and SVD, Forensic Science International, 233(1–3) (2013) 158–166.

[10] Lynch, F. Y. Shih, and H.-Y. M. Liao, An efficient expanding block algorithm for image copy-move forgery detection, Information Sciences, 239 (2013) 253–265.

[11] L. Li, S. Li, H. Zhu, and X. Wu, Detecting copy-move forgery under affine transforms for image forensics, Computers and Electrical Engineering, 40(6) (2014) 1951–1962.

[12] C.-M. Pun and K.-C. Choi, Generalized integer transform based reversible watermarking algorithm using efficient location map encoding and adaptive thresholding, Computing, 96(10) (2014) 951-973.

[13] X.-C. Yuan and C.-M. Pun , A Geometric Invariant Digital Image Watermarking Based on Robust Feature Detector and Local Zernike Moments, Proceedings of the 9th International Conference Computer Graphics, Imaging and Visualization, Hsinchu, (2012).