IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Analyse And Overview on Digital Image Tampering Detection Using Matlab

K. Manikantan

Dep. of Electronics and Communication Systems, AJK College of Arts and Science, Bharathiar University, Coimbatore, India

*Corresponding Author: manikandan.mother@gmail.com

Available online at www.ijcseonline.org

Accepted: 15/Aug/2018, Published: 31/Aug/2018

Abstract Modern digital technology and the availability of increasingly powerful image processing tools can easily manipulate the digital images without leaving obvious visual traces of having been tampered, so there is an urgent need to identify the authenticity of images. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In this paper going to see about different types of detection techniques are namely called as active methods, passive, cloning and splicing.

Keywords**:** Fragile Watermark, Semi fragile watermark, Passive Detection Method, Splicing Detection.

I. Introduction

Digital images are made of picture elements called pixels. Typically, pixels are organized in an ordered rectangular array. The size of an image is determined by the dimensions of this pixel array. The image width is the number of columns, and the image height is the number of rows in the array. Thus the pixel array is a matrix of M columns x N rows. To refer to a specific pixel within the image matrix, we define its coordinate at x and y. The coordinate system of image matrices defines x as increasing from left to right and y as increasing from top to bottom. Compared to normal mathematic convention, the origin is in the top left corner and the y coordinate is flipped. Image size is not to be confused with the size of the real world representation of an image. Image size specifically describes the number of pixels within a digital image. The real world representation of a digital image requires one additional factor called resolution. Resolution is the spatial scale of the image pixels. For example, an image of 3300x2550 pixels with a resolution of 300 pixels per inch (ppi) would be a real world image size of 11" x 8.5". To clarify resolution terms, ppi is pixels per inch and dpi is dots per inch. Ppi refers to pixel arrays, while dpi refers to printer resolution. In reality these two resolution terms are used interchangeably. Another resolution term you may encounter is ppi, for lines per inch, which describes halftone resolution and is used in magazine and newspaper printing. Many image editing applications default the resolution to 72 ppiImage tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. Figure 1 represented into types of detection techniques.

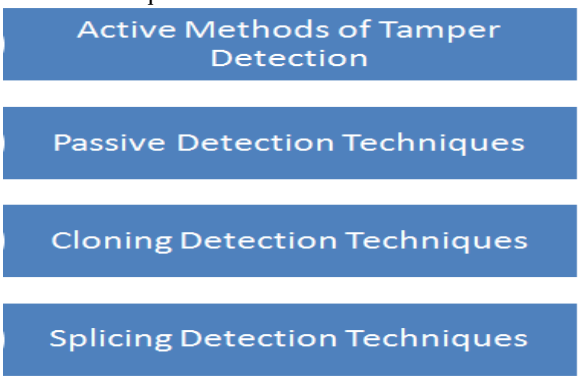

Figure 1: Detection Techniques

Nowadays altering digital images via intuitive software is an operation of simpleness with very low cost; thus every individual can synthesize a fake picture. For the widely accessible Internet, the false information disseminates extremely fast. As a consequence, the facts may be distorted and the public opinion may be affected, yielding negative social influence. It can be even worse in the justice when pictures are presented as evidence. Therefore, there is a strong demand for valid and robust authentication method to discern whether a picture is original or not. Two means are commonly utilized to make a forgery: copy-move and splicing. In the former case, a part of a picture is duplicated and then pasted onto other regions to cover any unwanted portion within the same picture. In the latter case, tampered image consists of two sources and retains the majority of one image for detail. Researchers and scientists have proposed many methods to expose such intended

manipulations. Passive forensic methods fulfill the task without additional information except for the image itself, thus showing advantages over active algorithms like watermarking and other signature schemas. The forged picture leaves some clues which can be used to locate the manipulated regions. In the practice of copy-move operation, because the pasted area, though it may probably be altered geometrically, shares some similar features with the original region which is duplicated, searching for analogous features abstracted from local area is a possible solution. SIFT feature can be used to locate clone areas. For splicing tampered image detection, considering that there may be some discrepancies between the host image and the spliced region attempts to find the difference to expose that forgeries make sense. For instance, Kakar et al. took advantage of motion blur discrepancy to detect fake pictures. For so many pictures stored or disseminated in JPEG format, some traces left by JPEG compression algorithm can be used.

II. Literature Survey

[1] **Dimpy Bansal, Sukhminder Kaushal(2016)** proposed detecting copy-paste forgery through quantitatively measuring lens radial distortion from one of a another parts of the image using line-founded calibration. Image forgery detection is a passive technique that uses the blind algorithm to detect or trace the image without any prior info or security codes. The images can be forged by splicing details from itself, which is called Copy-Move images, or spliced images. For Copy-Move images, copied regions in image can be post processed, rotated/flipped and scaled before pasting to other places to hide or remove any details. an adaptive support vector machine for the classification .This system is implemented using Matlab 2014a.For the purpose of detecting forgery, a set of original and altered images are given as input to the classifier. An efficient technique for detecting digital image forgeries is presented in this article which is dependent on method of illumination inconsistencies. As we all know that illumination inconsistencies present within the scene provide important cues for detecting false image. Right here the main point is to create an illuminate map from given images. These maps are then used to extract different edges situated and texture founded aspects. These aspects are additional processed in training and testing segment of classifier. An adaptive support vector machine is used to categorise whether given image as exact or cast.

[2] Mr. Soumen K. Patra, Mr. Abhijit D. Bijwe(2016) proposedan improved algorithm based on Singular Value Decomposition (SVD) to detect this image forgery. From time-to-time digital images have been mostly accepted as evidence of the depicted happenings. Because of dominant in computer field, business and many more field, adoption of digital image as authorized document has become frequent .The easiness of use and accessibility of image editing tools and low-cost hardware, makes it very easy to manipulate digital images without leaving any trace of tampering. Therefore we can't take the authenticity and integrity of digital images for granted. This challenges the dependability on digital images in medical diagnosis, as evidence in courts, as newspaper items or as legal documents because of difficulty in distinguishing original and modified contents. Digital Image Forensic is that branch of science which deals to expose the malicious image manipulation. Digital investigation field has developed to combat the problem of image forgeries in many areas like medical images, forensics, intelligence, etc. The original image is altered to get the tampered image; persons in an image have been masked by copying a region from the same image and pasting it over there. Post processing operation like blurring is used to diminish the effect of border inconsistencies between the two images. Detect copy-move forgery of different post-processing operations on snippet. Our method is a block-based and extracting SV feature. Copy-Move forgery is mostly used technique to create forgery in digital images. To perform indistinguishable copy-move forgery, post-processing of snippet is performed. Proposed algorithm can detect forgery under post-processing operations like rotation, scaling and noise. Proposed algorithm (SVD) has given a desirable output which is better than using PCA. SVD algorithm requires lower time than PCA in detection method. But as overlapping block size increases the total time required for detection decreases but false detection increases.

[3] **Manish Jain , Vinod Rampure(2017)** proposed an algorithm for digital image forgery for both joint photographic experts group (JPEG) and graphics interchange format (GIF). The digital image is 2D in x and y spatial plane. The intensity of the image at any point is determined by spatial coordinate. In this regard, capture, modify, compression, and generation operations are performed by converting the image into digital numbers such as 0s and 1s known as bits. The digital image is composed of a finite number of pixels. The size of the standard image, 1024x1024 pixel and 256 type colours are required 3MB of space in the RAM memory. Moreover, colours type image is required more size in RAM memory. In the digital world, cameras are utilized for video and image capture. In contrast to bright light, the camera's videos and images have saturation level is high. Consequently, when the dark light is saturation level is low. The saturation level lies between high and low when the light level is maintained. The image processing technique is highly used in such areas as biomedical, satellite, communication, electronics etc. In all these areas image features like compression, enhancement, and compression

are an open area of research, but all these features challenging task is forgeries phenomena happen. In a more formal way, forgeries image can be categories into two parts such as analogue and digital. In the type of analogue image the continuous signal treated, whereas digital type image has discontinuous signal treated. In fact, the digital image is popular nowadays in terms of quality of the image. The digital forgeries technique is a most used area of current research. The digital type forgery is most active research field with many benefits and threats with the consideration of complexity in the objective. As an algorithm, the authenticity of the image is performed on MATLAB R2015a (64bit) simulation tool.

[4] **Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom Gupta(2015)** proposed examined different type of image forgery and their detection techniques, mainly we focused on pixel based image forgery detection techniques. Imitations are not new to humanity but rather are an exceptionally old issue. In the past it was restricted to craftsmanship and writing yet did not influence the overall population. These days, because of the headway of computerized picture handling software and altering devices, a picture can be effortlessly controlled and changed. It is extremely troublesome for people to recognize outwardly whether the picture is unique or manipulated. There is fast increment in digitally controlled falsifications in standard media and on the Internet. This pattern shows genuine vulnerabilities and abatements the credibility of digital images. In this manner, creating procedures to check the honesty and realness of the advanced pictures is essential, particularly considering that the pictures are introduced as evidence in a court of law, as news things, as a part of restorative records, or as money related reports. In copy-move forgery (or cloning), some part of the picture of any size and shape is copied and pasted to another area in the same picture to shroud some important data as demonstrated. Pixel-based techniques accentuate on the pixels of the digital image. These techniques are generally classified into four sorts such as copy-move, splicing, resembling and statistical. We are concentrating just two sorts of techniques copy-move and splicing in this paper. This is most common image manipulation technique amongst the well-known phony identification techniques.

[5] **Sapna Sameria, Vaibhav Saran, A.K.Gupta(2015)** proposed digital techniques used in the forensic analysis of the various kinds of documents. The analysis of Documents through Digital Image Processing has been as old as forgeries started emerging through these software. With the dramatic growth and widespread applicability of digitalization of documents, the forensic questioned document community has encountered difficulty visualizing obliterated and altered handwriting using conventional methods. Over the past thirty years there has been a limited amount of research into using computers to enhance and automate the analysis performed by forensic document examiners. The technique of analysis of questioned documents for any alteration with the digital image processing is more accurate, non-destructive, faster and cheaper than other conventional methods of TLC and VSC. Thus, there is a need of a set of tools that can be applied to the image to check its authenticity and reach a conclusion to convince the court of law. Various Digital Image Processing software and its tools, even MATLAB, in the field of Handwriting analysis and various aspects of Image Forgery.

III. Detection Techniques

- Active Methods of Tamper Detection
- Passive Detection Techniques
- Cloning Detection Techniques
- Splicing Detection Techniques

3.1 Active Methods of Tamper Detection

Active taper detection techniques due to their inherent limitation, though, are not as common as those of the passive techniques still these are considered to be most efficient image authentication methods and a lot of research has been done in this field. These active image authentication techniques are commonly classified into two categories: the first method uses a fragile watermark, which localizes and detects the modifications to the contents. While the rate of tamper detection is very high for these methods they cannot distinguish between the simple brightness, contrast adjustments and replacement or addition of scene elements. Increasing the gray scales of all pixels by one would indicate a large extent of tampering by this method, even though the image content remains unchanged for allpractical purposes. The second method uses a semi-fragile watermarking, that only detects the significant changes in the image while permitting content-preserving processing. The fragile watermark though has good localization and security properties but cannot differentiate forgeries such as addition or removal of parts of image, from the innocent image processing operations such as brightness or contrast adjustments. Hybrid image authentication watermarking scheme that combines both the fragile and a robust watermark.

The hybrid watermark can be used to accurately pinpoint changes as well as distinguish forgeries from other innocent operations. Several researchers worked in these active tamper detection and authentication schemes and developed a number of fragile, semi-fragile, robust, public as well as private key basedwatermarks for copyright protection, authentication and tamper detection out of which, some either failed to effectively address the problems or sacrifice tamper localization accuracy of the original methods while

few of them were proved to be highly efficient and effective. However, the hierarchical digital watermarking method proposed by Prenatal is a simple but efficient method that not only localizes and detects tampering but also is capable of tamper recovery with a little degradation to the image quality. The precision of tamper detection and localization of this method is 99.6% and 100% after level-2 and level-3 inspection, respectively. The tamper recovery rate is better than 93% for a less than half tampered image.

3.2 Passive Detection Techniques

The passive methods are regarded as evolutionary developments in the area of tamper detection. In contrast to the active authentication techniques these methods neither require any prior information about the image nor necessitate the pre embedding of any watermark or digital signature into the image. The underlying assumption that is the basis of these schemes is, though the carefully performed digital forgeries do not leave any visual clue of alteration, they are bound to alter the statistical properties of the image. The passive techniques try to detect digital tampering in the absence the original photograph as well as without any pre inserted watermark just by studying the statistical variations of the images. Researchers of passive detection techniques generally focus on two types of passive methods, the copy-move forgery detection or cloning and splicing.

3.3 Cloning Detection

To clone or copy and paste a part of the image to conceal an object or person is one of the most commonly used image manipulation techniques. When it is done with care, it becomes almost impossible to detect the clone visually and since the cloned region can be of any shape and size and can be located anywhere in the image, it is not computationally possible to make an exhaustive search of all sizes to all possible image locations. Any Copy-Move forgery introduces a correlation between the original image segment and the pasted one which can be used as a basis for successful detection of this type of forgeries. Because the tampered image will likely be compressed and because of a probable use of the smoothing or other post processing operation, the segments may only match approximately not exactly. The authors in this paper give two different detection schemes: exact and robust matching those successfully detects duplicate regions in an image even when the images are post processed following a copy-paste. Methods based on blur movement invariants and DWT, SVD, PCA based sorted neighborhood.

3.4 Splicing Detection Techniques

Digital splicing of two or more images into a single image is another commonly used image manipulation technique. When performed carefully, the borders between the spliced regions can be visually imperceptible. It is a popular way to distort the semantic content of an image so as to fool the viewer to misbelieve the truth behind a scene. Image splicing is a fundamental operation in image forgery and is characterized by simple cut-and-paste operation that takes a part of an image and puts it onto either the same or another image without performing any post-processing smoothing operation such as edge blurring, blending to it. By Image tampering, it generally means splicing followed by the post-processing operations so as to make the manipulation imperceptible to human vision. Splicing detection is more challenging in comparison to cloning detection as unlike cloned images spliced images do not have any duplicate regions and unavailability of the source images offer no clue about the forgery. In however, the authors have shown that splicing disrupts higher-order Fourier statistics, which can subsequently be used to detect splicing. splicing detection approach based on a natural image model that consists of statistical features extracted from the given test image as well as 2-D arrays generated by applying multi-size block DCT transform to the test images. With the assumption that fusion of multiple statistical features can improve the performance of splicing detection. new splicing detection approach based on the features utilized for steganalysis. They merge Markov process based features and DCT features for splicing detection. The proposed approach achieved up to 91.5% accuracy with a 109-dimensional feature vector. A novel method for detecting image splicing by thresholding transition region measures of DWT coefficients of a suspicious image in chroma spaces. Only the low frequency sub-band of the DWT of the suspected image is extracted to reduce the size of the image and improve the performance. Because splicing combines image parts from multiple images so, careful study of the lighting conditions can provide a better clue on detection of these types of manipulations.

IV. Conclusion

Due to considerable improvement in computing and network technologies, and the availability of better bandwidths, the past few years have seen a considerable rise in the accessibility, sophistication, and transmission of digital images using imaging technologies like digital cameras, scanners, photo-editing, and software-packages. In this paper analyzedsome techniques for enhance the image tampering.Each one technique have some performanceratio not only the advantages and also have somedrawbacks within that. In future work will choose any one technique which is most secure and suitable to do betteraccuracy for image tampering process and then applysome enhancement within that to proof much better thanthe old performance.

References

[1] Dimpy Bansal, Sukhminder Kaushal," A Novel Analysis Of Image Forgery Detection Using SVM", International Journal Of Engineering And Applied Sciences (Ijeas) Issn: 2394-3661, Volume-3, Issue-12, December 2016.

[2] Mr. Soumen K. Patra, Mr. Abhijit D. Bijwe," Copy-Move Image Forgery Detection Using Svd", International Research Journal Of Engineering And Technology (Irjet).

[3] Manish Jain , Vinod Rampure," Algorithm For The Digital Forgery Catching Technique For Image Processing Application", International Journal Of Advancement In Engineering Technology, Management And Applied Science (Ijaetmas).

[4] [13] Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom," An Evaluation Of Digital Image Forgery Detection Approaches", International Journal Of Applied Engineering Research, Issn 0973-4562 Volume 12, Number 15 (2017) Pp. 4747–4758.

[5] Sapna Sameria, Vaibhav Saran, A.K.Gupta," A Review Of Trends In Digital Image Processing For Forensic Consideration", Ijournals: International Journal Of Software & Hardware Research In Engineering Issn-2347-4890.

[6] Harpreet Kaur1 , Jyoti Saxena2 And Sukhjinder Singh," Simulative Comparison Of Copy- Move Forgery Detection Methods For Digital Images", International Journal Of Electronics, Electrical And Computational System Ijeecs Issn 2348-117x.

[7] Sini P Somanathan, D Jude Hemanth, Jisi C And Jyothi M," Forgery Detection In Digital Images Using Clustering Techniques", International Conference On Security And Authentication - Sapience14.

[8] Amandeep Kaur, Vaibhav Saran, A. K. Gupta," Digital Image Processing For Forensic Analysis Of Fabricated Documents", International Journal Of Advanced Research In Science, Engineering And Technology.

[9] Jobin Abraham," A Blind Watermarking Scheme For Tamper Detection In Digital Images", Ictact Journal On Image And Video Processing, November 2015, Volume: 06, Issue: 02.

[10] Mrugesha Lad , Naresh Patel," Passive Digital Image Forgery Detection Techniques And Implementation", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering Vol. 4, Issue 5, May 2016.

[11] Thuong Le-Tien, 1marieluong, 2tu Huynh-Kha, Long Pham-Cong-Hoan, An Tran-Hong," Block Based Technique For Detecting Copy-Move Digital Image Forgeries: Wavelet Transform And Zernike Moments", Proceedings Of The Second International Conference On Electrical And Electronic Engineering, Telecommunication Engineering, And Mechatronics, Philippines 2016.

[12] Mrs.Nisha , Mr. Mohit Kumar," Review Of Copy Move Forgery With Key Point Features",,International Journal Of Advance Research , Ideas And Innovations In Technology.

[13] Yadwinder Kaur, Dr. Sukhjeet Kaur Ranade," Image Authentication And Tamper Detection Using Fragile Watermarking In Spatial Domain", International Journal Of Advanced Research In Computer Engineering & Technology (Ijarcet) Volume 6, Issue 7, July 2017, Issn: 2278 – 1323.

