IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 8, August 2016

A Review Paper on Forgery Part Detection using Different Methods

Manpreet Kaur[1], Mandeep Kaur[2]

CSE Department, GKU, Bathinda[1, 2]

Abstract: Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. Digital image forensics aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. Nowadays, thanks to the promising results attained by early studies and to the always growing number of applications, digital image forensics represents an appealing investigation domain for many researchers. Fake images are many times used to publicize in social Medias and news papers. Many cases are noted in regard to the defaming business as well as political leaders by using fake photos and videos. In this paper DWT and Shift technique is used with optical flow to detect the video forgery frames and different parameters are calculated.

Keywords: Frame, Video, forgery, DWT and SIFT etc.

I. INTRODUCTION

A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. Without qualifications, the term "digital image" usually refers to raster images also called bitmap images.When we see a picture on our monitor or use our digital camera (or scanner), the image we are viewing or dealing with is not continuous like a pencil drawing – it is made up of many small elements next to each other. When we have enough elements, we get the illusion of a picture or image. Early digital images (before color) appeared in black and white. The tiny elements that comprised digital images were either black or white. These two ‘colors’ corresponded to 1 and 0 (called BITS or BI-nary digits). Digits 1 and 0 are used in the binary (base 2) system. Thus, a map (pattern) made up of these 1’s and 0’s was referred to as a bit-map. All digital images are a rectangle or square. Today, the elements are called pixels.

Forensics means the use of science and technology in the investigation and establishment of facts. So the photographs or other pictures can be transmitted to and reconverted into pictures by another computer. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of Material found in digital devices. Digital image forensics aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. Nowadays, thanks to the promising results attained by early studies and to the always growing number of applications, digital image forensics represents an appealing investigation domain for many researchers. With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users. Image manipulation has become commonplace with growing easy access to powerful computing abilities. Some common image manipulation with the intension of deceiving a viewer includes:-

- Copy and paste
- Composition or Splicing
- Retouching, healing, cloning
- Content embedding or steganography

One of the most common types of image forgeries is the copy-paste forgery, wherein a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. In Figure1, an example of copy-move forgery can be seen where the original image (Figure 1(a)) has one bird flying in the sky whereas in forged one (Figure (b)), Cloning tool of Photoshop has been used to show that there are two birds flying.

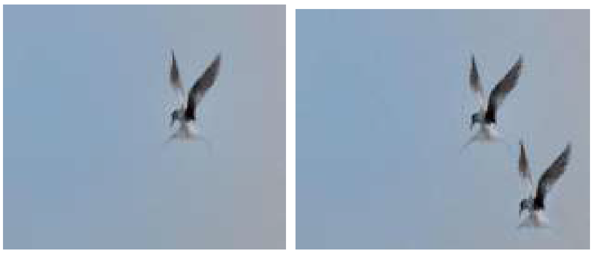

Figure1. Example of Copy-Move forgery (a) original image (b) tampered image

DOI 10.17148/IJARCCE.2016.5895

So, Digital image forensics aims at restoring some of the lost trustworthiness of digital images and revolves around the following two fundamental questions:

- Where is the image coming from?
- (How) Has the image been processed after acquisition?

In this work, we show that with the exception of the identity mapping, pixel value mappings leave behind statistical artifacts which are visible in an image's pixel value histogram. We refer to these artifacts as the intrinsic fingerprint of a pixel value mapping. By observing the common properties of the histograms of unaltered images, we are able to build a model of an unaltered image's pixel value histogram. We then use this model to identify diagnostic features of a pixel value mapping's intrinsic fingerprint. Because a number of image processing operations are in essence pixel value mappings, we propose a set of image forgery detection techniques which operate by detecting the intrinsic fingerprint of each operation. Specifically, we propose methods for detecting general forms globally and locally applied contrast enhancement, as well as a method for identifying the use of histogram equalization, a commonly used form of contrast enhancement.

Additionally, we propose a method to detect the global addition of noise to a previously JPEG-compressed image by detailing the effect of noise on the fingerprint of a known pixel value mapping applied to the image in question.Whilemuchofthisworkfocusesondetectingoperationswhichalter the perceptual qualities of an image as opposed to more obviously malicious tampering, detecting the image manipulations discussed in this work is still forensically significant. The detection of globally applied contrast enhancement provides insight into an image's processing history and may be useful prior information for other detection algorithms. Furthermore, contrast enhancement operations may be locally applied to disguise visual clues of image tampering. Localized detection of these operations can be used as evidence of cut-and-paste type forgery. Additive noise may be globally applied to an image not only to cover visual evidence of forgery, but also in an attempt to destroy forensically significant indicators of other tampering operations. Though the detection of these types of operations may not necessarily pertain to malicious tampering, they certainly throw in doubt the authenticity of the image and its content.

II. CURRENT ISSUES

Since the digital images play a significant role in simplifying the way of representing and transferring ideas flexibly, an attention has been paid recently towards investigating the suitable mechanism for analyzing and detecting forgery in the digital images. This attention was due to the latest malicious activities in which a single object inside the image is duplicated within the same image. Such activities can be seen in the copy-move forgery that considers one of the most known activity aims at including or hiding a [13, 14]. Many scholars have agreed that copy-move forgery works on the premises of detecting added noise, color changes, and texture that can be found within the duplicated area inside the image. Usually it is possible to identify the duplicated object by computing and comparing these premises with the whole image. But new forgery detection techniques are still lacking of up to date malicious activities. Such assumption came from the ability of forgers to change the geometry of the duplicated object easily by modifying the image's features. Therefore, a new copy-move forgery detection technique is needed in order to balance the new malicious activities on digital images [15, 16].The issues and challenges being addressed in the domain of digital image forgery are forgery detection techniques, digital forgeries of social impacts, and forgery prevention techniques. The digital forgeries have many perspectives and implications on social, legal, technical, intelligence, investigative mechanisms, security, managerial issues [17,18].

The forgery creation and detection are complimentary to each other. Figure 1 presents the workflow of the common forgery detection technique consists of four faces, these are overlapping blocks, feature extraction, block matching, and forgery decision. The utilization of this method to detect new forgery activities is considered to be useless, the reason back to that foragers have developed a new ways to overlap objects within the original image, this process of forgery creation contributes to the advances and sophistication in forgery detection methods which still challenging topic. From the other hand, the confidentiality involved in the current forgery approaches presents a new level of complexity in forgery creation and forgery detection processes and acts as a hindrance to both of these processes. Figure 1 shows the general forgery detection approach consists of overlapping blocks, feature extraction, block matching, and forgery decision. This approach allows applying several extraction techniques such as DCT, PCA, etc. It also allows applying different matching techniques such as K-D tree and radix sort.

III. FORGERY DETECTION

Forgery detection methods become much more complicated to deal with the latest forgery techniques. This back to the availability of digital editing tools, alteration, and manipulation become very easy and as a result forgery detection becomes a complex and threatening problem [13]. Image forgery detection can be manipulated in various ways with many simple operations like affine transforms such as translation, scaling, etc., compensation operations such as brightness, colors, contrast adjustments, etc., suppression operation such as noise extraction, filtering, compression, etc., [9].Furthermore, more complex operations are also possible such as compositing, blending, matting, cropping, photomontage leading to visually untraceable artifacts in an image [14]. The automatic and scientific method of detecting the forged images has become a big challenging

DOI 10.17148/IJARCCE.2016.5895

problem for researchers and the same problem is true for every multimedia contents.

IV. BRIEF LITERATURE SURVEY

Several reviews of the literature on image retrieval have been published, from a variety of different viewpoints.

Tushant A. Kohale et al. **[2014]** have studied Digital images are the most important source of information transfer. The availability of powerful digital image processing software's, makes it relatively easy to create digital forgeries from one or multiple images. In today's world it is easy to manipulate the image by adding or removing some elements from the image which result in a high number of image forgeries. A copy-move forgery is created by copying and pasting content within the same image, and potentially post-operating it. The detection of copy-move forgeries has become one of the most actively researched topics in blind image forensics. The key objectives of the proposed approach is to study the effect of different types of tampering on the digital image, detect image forgery by copy-move under many types of attacks by combining block-based and feature based method and accurately locating the duplicated region[14].

Salma Amtullah et al. **[2014]** studied Tampering in digital images has become very easy due to the availability of advanced image editing software's to the users. Images are being tampered in a very efficient manner without leaving any visual clue. As a consequence, the content of digital images cannot be taken as for granted. There are various types of image tampering techniques. One of the most common tampering techniques is copy-move forgery. In copy-move forgery one part of an image is copied and pasted in another part of the same image. In this paper, the passive image forensic method is presented to detect copy move forgery in digital images. The proposed method is based on SURF (Speed Up Robust Features) algorithm. In this method the features are extracted and their descriptors are obtained by SURF algorithm and the Nearest Neighbor approach is used for feature matching to identify the copy move forgery in digital images. This detection method is found to be rotation and scale invariant and is robust enough to noise, jpeg compression and blurring. Multiple copy move forgery is also detected by this method[15].

I. Amerini et al**. [2011]** One of the principal problems in image forensics is determining if a particular image is authentic or not. This can be a crucial task when images are used as basic evidence to influence judgment like, for example, in a court of law. Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on scale invariant features transform (SIFT) is proposed. Such a method allows us to both understand if a copy–move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning. Extensive experimental results are presented to confirm that the technique is able to precisely individuate the altered area and, in addition, to estimate the geometric transformation parameters with high reliability. The method also deals with multiple cloning.

P. Kakar et al. **[2012]** Image manipulation has become commonplace with growing easy access to powerful computing abilities. In this paper, the author propose a novel technique based on transform-invariant features. These are obtained by using the features from the MPEG-7 image signature tools. Results are provided which show the efficacy of this technique in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring. We obtain a feature matching accuracy in excess of 90% across post processing operations, and are able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art[2].

S. Bayram et al. **[2006]** A part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. Hence, the goal in detection of copy-move forgeries is to detect image areas that are same or extremely similar. In this paper, the author review several methods proposed to achieve this goal. These methods in general use block-matching procedures, which first divide the image into overlapping blocks and extract features from each block, assuming similar blocks will yield similar features. Later, a matching step takes place where the aim is to find the duplicated blocks based on their feature vectors. A forgery detection decision is made only if similar features are detected within the same distance of features associated to connected blocks. The author examine several different block based features proposed for this purpose in relation to their time complexity and robustness to common processing scaling up/down, compression, and rotation[3].

A.N. Myna et al. **[2010]** As result of powerful image processing tools, digital image forgeries have already become a serious social problem. In this paper he describe an effective method to detect Copy-Move forgery in digital images. Our technique works by first applying DWT (Discrete Wavelet Transform) to the input image to yield a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. Due to DWT usage, detection is first carried out on lowest level image representation. This approach drastically reduces the time needed for the detection process and increases accuracy of detection process.

M.C. Stammn et al. **[2010]** As the use of digital images has increased, so has the means and the incentive to create digital image forgeries. Accordingly, there is a great need for digital image forensic techniques capable of detecting image alterations and forged images. A number of image processing operations, such as histogram equalization or gamma correction, are equivalent to pixel value mappings. In this paper, the author show that pixel value mappings leave behind statistical traces, which we shall refer to as a mapping's intrinsic fingerprint, in an image's pixel value histogram. Then they propose forensic methods for detecting general forms globally and locally applied contrast enhancement as well as a method for identifying the use of histogram equalization by searching for the identifying features of each operation's intrinsic fingerprint. Additionally, we propose a method to detect the global addition of noise to a previously JPEG-compressed image by observing that the intrinsic fingerprint of a specific mapping will be altered if it is applied to an image's pixel values after the addition of noise[7].

Dhara Anandpara et al. **[2012]** With advent of many powerful editing tools in the digital image processing, image forgery is the big concern today in Digital Forensics Industry. Image forgery can be apply either in single image by coping some region of image and pasting it to another place in the same image or in composite image by combining two or more images together. The focus of my research work is to develop a forensic system to detect both type of forgery within a single place. Many Copy-move Forgery Detection (CMFD) algorithms have been developed to detect forgery within single image but are not robust to geometric transformation. Double JPEG compression is used extensively for localization of regions for composite images forgery such as Image Slicing, In-painting etc. A proposed system is a fusion based system which will allow to detect the image tampering using both techniques i.e. CMFD and DJPG. This gives insights of using both image detection algorithms within same image and in single framework so that detection is evident at single place. A system will compute a likelihood map to indicate the forged area that is accrued due to Copy. To reduce computational cost of system features are extracted from taking the mean value of DCT (discrete cosine transform) coefficients. The proposed scheme is not only robust to copy-move forgery, but also to blurring or nosing adding and with low computational complexities [16].

V. PROBLEM FORMULATION

Digital image forensics aims at validating the authenticity of images by recovering information about their history. Copy-paste forgery, where in a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. Due to the availability of higher solution digital cameras, hi-tech personal computers, powerful software and hardware tools in the image editing and manipulating field, it become possible for someone to create, alter and modify the contents of a digital image and to violate its validation. Fake images are many times used to publicize in social Medias and news papers. Many cases are noted in regard to the defaming business as well as political leaders by using fake photos and videos. The problem of detecting if an image has been forged is investigated; in particular, attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create duplication or to cancel something that was awkward. The photomontage detection problem, one of the fundamental tasks is the detection of image splicing. Image splicing assumes cut and paste of image regions from one image onto another image. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of images or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue.

Techniques Comparison Table

Name of Technique	Advantage	Disadvantage
DWT	It is used to split the image into different frequency bands. So that we can easily process the particular block of the image and video frame.	It is not split the image in to maximum level of the image.
SIFT	Sift technique is used to process the frame and image with the help of neighboring pixel values.	In the sift technique we cannot get the exact value of the pixels and we are not finding the exact route of the processing of frames.
Optical Flow	It is used to process the frame with the help of object motion where we have to find the forgery part.	Sometimes it is unable to find the exact flow of the processing of the objects.

VI. CONCLUSION & FUTURE WORK

In this paper I have studied different researchers' research work. Each and every author studied different problems and different techniques, but I have founded some problems in the video forgery detection. In the video some frames are forgery frames. The problem of detecting if an image has been forged is investigated; in particular,

DOI 10.17148/IJARCCE.2016.5895

attention has been paid to the case in which an area of an image is copied and then pasted onto another zone to create duplication or to cancel something that was awkward. In the future work I will use DWT and SIFT technique with optical flow to detect the forgery from the video frames and some parameters are calculated to check the performance of the work.

REFERENCES

[1]. S.Khan and A.Kulkarni ,"Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010.

[2]. P.Kakar and N.Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.

[3]. S.Bayram, H.T.Sencar and N.Menon"A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.

[4]. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.

[5]. M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.

[6]. M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.

[7]. M.C.Stamnn,"Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security , vol. 5 No 3, 2010.

[8]. M. Chen, J. Fridrich, M. Goljan, and J. Luká˘s, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[9]. T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," in Proc. ACM Multimdedia, Singapore, 2005, pp. 239–248.

[10]. M. K. Johnson and H. Farid, "Exposing digital forgeries in complexlighting environments," IEEE Trans. Inf. Forensics Security, vol. 2, no.3, pp. 450–461, Sep. 2007.

[11]. M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Multimedia and Security Workshop, New York, NY, 2005, pp. 1–10.

[12]. T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Proc. IEEE Int. Symp. Circuits Systems, Vancouver, BC, Canada, May 2004, vol. 5, pp. V-688–V-691.

[13]. S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, p. 041102, 2006.

[14]. Tushant A. Kohale*, Prof. P. R. Lakhe " Detection of Postoperated Copy Move Image Forgery by Integrating Block Based and Feature Based Method" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.

[15]. Salma Amtullah, Dr. Ajay Koul " Passive Image Forensic Method to detect Copy Move Forgery in Digital Images" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 96-104.

[16]. Dhara Anandpara" A Joint Forensic System to Detect Image Forgery using Copy Move Forgery Detection and Double JPEG Compression Approaches" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[17]. Pan, X. Z., & Wang, H. M. (2012). The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA.Advanced Materials Research, 532, 692-696.

[18]. Shiva kumar, B., & Baboo, S. S. (2011). Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors. International Journal of Computer Applications, 27(3).

[19]. Yao, H., Qiao, T., Tang, Z., Zhao, Y., & Mao, H. (2011).Detecting Copy-Move Forgery Using Non-negative Matrix Factorization. Paper presented at the Third International Conference on Multimedia Information Networking and Security (MINES).

[20]. Pujari, V. S., & Sohani, M. (2012b). A Comparative AnalysisOn Copy Move Forgery Detection Using Frequency Domain Techniques. International Journal of Global Technology Initiatives, 1(1), E104-E111.

[21]. Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J. (2013).Region duplication detection based on Harris corner point sand step sector statistics. Journal of Visual Communication and Image Representation, 24(3), 244-254.

[22]. Liu, M.-H., & Xu, W.-H. (2011). Detection of copy-moveforgery image based on fractal and statistics. Journal ofComputer Applications, 8, 061.

[23]. Yadav, P., Rathore, Y., & Yadu, A. (2012). DWT BasedCopy-Move Image Forgery Detection. International Journalof Advanced Research in Computer Science and ElectronicsEngineering (IJARCSEE), 1(5), 56-58.

[24]. Pujari, V. S., & Sohani, M. (2012a). A Comparative Analysison Copy Move Forgery Detection in Spatial Domain MethodUsing Lexicographic and Non Lexicographic techniques.IJECCE, 3(1), 136-139.

[25]. Shiva kumar, B., & Santhosh Baboo, L. D. S. (2010).Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology, 10(7).

DOI 10.17148/IJARCCE.2016.5895