Performance Evaluation of Forgery Detection of JPEG Compression

Vishalkumar J Vankar[1], Krunal J. Panchal[2]

[1]Research Scholar, Computer Engineering Department, L.J. Institute of Engineering & Technology, Gujarat, India
[2] Assistant Professor ,Computer Engineering Department, L.J. Institute of Engineering & Technology, Gujarat, India

ABSTRACT

Now today's Digital world Digital images have a very significant role in various fields like medical imaging, journalism, criminal and forensic investigations. but now a day's the advent of image editing and processing tools it is conceivable to alter digital images very easily without leaving any obvious tampering traces. Thus, image forgery has become very easy and authenticity of digital images has been severely threatened. we are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Most common operations that are involved in the creation of forged images are contrast enhancement, copy-paste forgery, copy- create forgery etc. so in this survey paper some methods are represent forgery detection techniques. Paper includes a DCT compression for forge region detection, feature extraction and contrast enhancement and block matching method for forgery detection. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images

Keywords :- *Forgery, DCT compression, Contrast Enhancement, splicing, BAG.*

1. INTRODUCTION:

Now a days image forgeries are common problems as we know the image forgery can be done by using simple image editing tools such as Windows Image editor, GIMP image editor and Photoshop etc. So it is very difficult to decide the given image is original or forged one with our naked eye and as we know it is very much important to identify an unforged image to take a right decisions.

- Types of Digital image forgery:
  1. Image Retouching: this is a less harmful than a other forgery methods. In this method certain features or parameters of the image are enhanced or degraded.[5]
  2. Image Splicing: most common manipulation method. In this method forgery can be defined as a cut-and paste of image regions from one image onto the same or another image without post processing.[5]
  3. Cloning: in which certain portions of the image are copy pasted in the same image to conceal a person or objecting the scene.[5]

Fig -1: Example of Forgery[4]

- Digital images forgery detection approaches:
  1. Active approaches**:** certain information is embedded inside an image during the creation or before the image is being disseminated to the public Example: Water marking[5]
  2. Passive approaches: Passive method does not require any pre-image distribution information which is to be inserted into a digital image. Example: JPEG compression, Wavelet transformation[5]

2. LITERATURE REVIEW:

2.1 Performance Evaluation of Forgery Detection of JPEG Image Compression

- In [1] Dr.M.Anto Bennet, G.Sankar Babu, R.Kaushik K, B.S.Jayavignesh paper proposed a forensic algorithm to discriminate between original and forged regions in JPEG images, under the hypothesis that the tampered image presents a double JPEG compression, either aligned (ADJPG) or nonaligned (NA-DJPG). A method is a based on the he derivation of a unified statistical model characterizing the DCT coefficients when an aligned or a nonaligned double JPEG (A-DJPG or NA-DJPG) compression is applied ,the statistical model is used for the generation of a likelihood map that shows the probability of each 8x8 image block of being doubly compressed. The validity of the proposed system has been demonstrated by computing the ROC curves and the corresponding AUC values for the double compression detector based on properly thresholding the likelihood map. The effectiveness of the proposed method is also confirmed by tests carried on realistic tampered images.

2.2 Revealing Image Forgery through Image Manipulation Method

- In [2] Ms. Jayshri Charpe, Ms. Antara Bhattacharya paper are forgery detect using two method. First method is global contrast enhancemen detection. In this algorithm proposed for global contrast enhancement detection in this paper is robust against the post processing operation such as JPEG compression. Second method is a copy-paste forgery detection in this method algorithm is proposed to detect the copy-paste forgery created using single source image. Here, we used the DCT for extracting the feature in order to detect the forged image. The proposed technique can efficiently detect the large block size areas up to size 64*64.

2.3 Paint-Doctored JPEG Image Forensics Based on Blocking Artifacts

- In [3] Ali Ebrahimi, Subariah Ibrahim, Eghbal Ghazizadeh, Mojtaba Alizadeh propose a passive method for detecting painted areas on widely used JPEG images is proposed. The block processing during JPEG compression presents horizontal and vertical breaks into images, which is recognized as block artifact grids (BAGs). The detection technique is based on the fact that BAGs usually disarrange after performing painting operations. extensively used JPEG standard, the blocking processing presents horizontal and vertical breaks into images, which is recognized as block artifacts grids (BAGs). This phenomenon is typically preserved as flaw of JPEG, and many efforts have been done to estimate it or to weaken it.

Though, the block artifact is used in the proposed method to indicate whether an image is manipulated or not. To achieve the objective, the block artifact grid must be extracted initially as clearly as possible.

2.4 Image Forgery Detection Using Feature Based Clustering in JPEG Images

- In [4] Gunjan Bhartiya, Anand Singh Jalal paper a very simple and effective method is presented which uses the analysis of histograms of doubly compressed images and some features in the histogram are then utilized in order to differentiate the doubly compressed area from that of singly compressed area. The method is effective in the sense that it can detect forged region accurately and at the same time, it is computationally more efficient as opposed to the previous techniques of forgery detection. It uses a feature based clustering on the grayscale version of the image which makes computationally efficient. It classifies the area of the image as original or tampered based on feature computed on the histogram of a doubly compressed JPEG image.

2.5 Detection of Splicing Forgery Using Wavelet Decomposition

- In [5] Abhishek Kashyap, B. Suresh, Megha Agrawal, Hariom Gupta, Shiv Dutt Joshi proposed a new method for splicing type of image forgery detection. This method is based on wavelet decomposition and block matching, which is describe below. In this method, first take a forged image for analysis purpose, then we follow the main step: (i) wavelet decomposition of an input image; (ii) block matching; (iii) Duplicated regions map creation. this proposed algorithm detect copy-create forgery shows better performance with tampered images independent of noise or contrast changes in the copied areas. We can process larger size images with reduced time complexity, as we know that there are many ways to create, alter, and digitally manipulate any given image,and the accuracy of a detection method is influenced by the amount of compression and subsequent recompression, file size of the image.

3. COMPARATIVE TABLE:

Table -1: Comparative Table

Paper Title	Methods/Techniques	Advantages	Disadvantages
Performance Evaluation of Forgery Detection of JPEG Image Compression	Complexity Forensic Algorithm	Effective for realistic tempered images	No valid for Resizing are applied between two compression
Revealing Image Forgery through Image Manipulation Method	DCT based Feature extraction method	Detect the large duplicate areas up to 64*64 blocks	Less Accurate for Compression

Paint-Doctored JPEG Image Forensics Based on Blocking Artifacts	Blocking Artifact grids(BAGs)	Effective for Image Manipulation	BAGs images not clear
Image Forgery Detection Using Feature Based Clustering in JPEG Images	Classification, Clustering	Better Accuracy, Provide better result than probability based approach	Not work well for non-natural image
Detection of Splicing Forgery Using Wavelet Decomposition	Wavelet Decomposition, Block Matching	independent of noise or contrast changes	Not worked for scale or rotated copy create image

4. CONCLUSION:

The research methodology for JPEG image forensic it seems that existing approach are based on only block wise and contrast based According to paper analysis number of methods and technique use for compression and Forgery detection. But still some problems like detection , noise, pixel sparse, attacks, false alarm rate.

5. REFERENCES:

[1]. Dr.M.Anto Bennet, G.Sankar Babu, R.Kaushik Krishna and B.S.Jayavignesh "Performance analysis of forgery detection of JPEG image compression" IEEE 2015 Online International Confernece on Green Engineering and Technologies (IC-GET 2015), DOI:10.1109/GET.2015.7453773, Pages:1-12

[2]. Ms. Jayshri Charpe and Ms. Antara Bhattacharya "Revealing Image Forgery through Image Manipulation Method" Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015), DOI: 10.1109/GCCT.2015.7342759, Volume: 23, Issue: 11, Nov. 2016, Pages:723-727

[3]. Ali Ebrahimi, Subariah Ibrahim, Eghbal Ghazizadeh and Mojtaba Alizadeh" Paint-Doctored JPEG Image Forensics Based on Blocking Artifacts" Computing and Communication(IEMCON)2015 international conference and Workshop on, DOI: http:10.1109/IEMCON.2015.7344427, Pages:1-5

[4]. Gunjan Bhartiya, Anand Singh "Image Forgery Detection Using Feature Based Clustering in JPEG Images" 2014 9th international conference on industrial and information system , DOI: 10.1109/ICIINFS.2014.7036583 Pages: 1-5

[5]. Abhishek Kashyap, B. Suresh, Megha Agrawal, Hariom Gupta, Shiv Dutt Joshi" Detection of Splicing Forgery Using Wavelet Decomposition" IEEE international conference on computing, communication, automation, DOI: 10.1109/CCAA.2015.7148492, Volume: 26, Issue: 9, Sept. 2016, Pages:843-848

[6]. Vincent Christlein," An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions On Information Forensics And Security, 2011.

[7]. G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images," IEEE Trans. Inf. Forensics Security, Mar. 2014.