IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 3, Ver. II (May.-June. 2017), PP 97-101
www.iosrjournals.org

A Survey on Image Tempring Using Various Techniques

Nisha Chauhan[1], Arun Agarwal[2]
[1]*Research scholar, Deptt. Of Computer Science & Engg. ITM Group Of Institutions, Gwalior(M.P.)*
[2]*Assistant Professor, Deptt. Of Computer Science & Engg. ITM Group Of Institutions,Gwalior(M.P.)*

Abstract*: Digital images can be easily tampered with image editing tools. The detection of tampering operations is of great importance. Passive digital image tampering detection aims at verifying the authenticity of digital images without any a prior knowledge on the original images. There are various methods proposed in this filed in recent years. In this paper, we present an overview of these methods in the first part, various image forgery detection techniques are classified and then an overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed.*

Keywords*: Image tampering, Active approach, Passive approach, copy-move, forgery;*

I. Introduction

With the advancement in information technology and imageprocessing software the manipulation of the images has increased considerably from past few years. Internet has further facilitated the availability of various images processing software. Even an amateur can create forged images for playful purpose. Image forgery has a long history and hisexploitation is done usually for some specific purpose. It may be done to hide some content from the image or to alter the contents by combining it with other images.[1]

Sometimes intruder creates a tampered image that seems like original using powerful image editing softwares. The purpose of such images may be for creating some thrilling news, misleading information, etc. These images highly impact social, political and business environment.

Basically, the image tampering detection techniques are based on two type of approaches i.e. active and passive (blind). In former detection techniques the credibility is assured by using pre-embedded digital watermark or digital signature.[2]

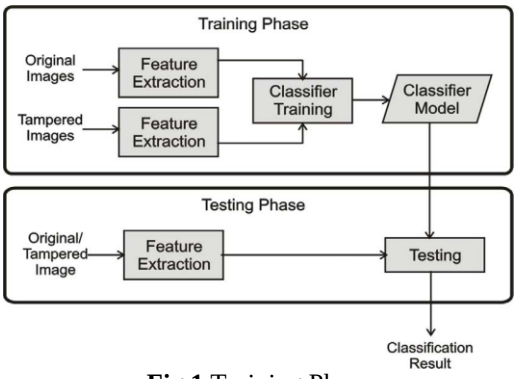

Fig.1 Training Phase

The progress of highly sophisticated digital photo editing software, digital images now becomes easy to manipulate.It difficult to see the changes in naked eyes. The common use of digital social media enables a person to share and upload any kind of images to the Internet.[3]

The most common type of fraud is an attack on the content of an image. It is often called Copy-Paste, Copy- Move or Collage attack, when one of the parts of the image is copied to another part of the same or a different image, thereby altering the original content.[4]

II. Image Tampering

To detect image tampering, we should know about image tampering operation itself first. In, the digital forgery operation isdivided into six different categories: compositing, morphing, re-touching, enhancing, computer generating and painting. In fact, almost all state-of-the-art tampering detection technique aims at compositing operation. With powerful image editing tool (e.g. Photoshop or lazy snapping), compositing tampered images is much easier and can result in much more realistic images. Image tampering involves the selection, transformation, composition of the image fragments and the retouching of the final image. Here, we want to highlight that a tampered image means part of the content of a real image is altered. This concept does

not include those completely synthesized images, e.g. images completely rendered by computer graphics or by texture synthesis. In other words, an image is tampered implies that it includes into two parts: the authentic part and the tamperedpart. All the algorithms introduced later focus on the tampered images defined here. [5].

III. Classification Of Image Forgery Techniques

Image forensics techniques are divided into two types: one is active protection, and the other is passive detection. Which again consist of many different methods?

A. Active Approach**,** In this approach, the digital image requires some kind of pre-processing like watermark embedded or signatures are generated at the time of creating the image. We can detect the Image is tampered, if special information cannot be extracted from that obtained image. Watermarking is such a way of active tampering detection, as a security structure is embedded into the image, but most present imagingdevices do notcontain any watermarking or signature module and that are similar to the application of active protection.[6]

Techniques under this group are also known as informed approach. These techniques use in-built construct to provide security to the image. Image tampering is detected using following methods:

1) Data hiding approach: In this approach, the secondary data embedded into the image.

*2) Digital signature:*Image hash functions are used to generate image hash value which is depends on the unique features of image. Image hash value is associated with or embedded into image for checking image integrity.

B. Passive image forensics is generally a great challenge in image processing techniques. There is not a particular method that can treat all these cases, but many methods each can detect a special forgery in its own way. Neither construct is embedded in the image and nor linked with it for security, as like active approaches and hence this method is also known as raw image analysis.

In these techniques image semantics are used to tamper detection without of any prior information, therefore these are also known as raw image analysis or blind tamper detection.

The criteria used to perform passive tamper detection are listed as below:

- Physical and semantic inspection
- Light inconsistency analysis
- Detection of duplicate regions
- Analysis of sensor inherited noise
- Retrieval of camera response function
- Double compression[7]

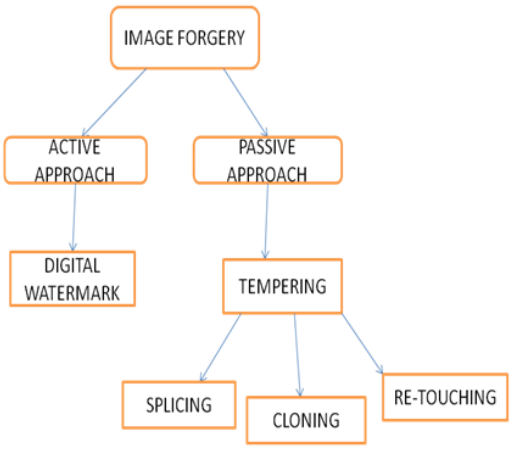

Fig. 2 Classification of image forgery [8]

1. Digital watermarking

Watermarking can be defined as process of hiding the digital information.

In entire process of water marking has three major steps are include like embedding, attack and detection. In the process of embedding with the help of watermark signal and host signal i.e. original data we always used to generate watermark signal. Then over the transmission media watermark signal transmitted to receiver from sender.[9]

2. Tampering– Tampering is manipulation of an image to achieve a specific result is known as tampering.

Fig.3 Tampering

Tempering is divided into three parts:

- SPLICING
- CLONING
- RE-TOUCHING

1) **Splicing (Compositing)**- A common form of photographic manipulation in which the digital splicing of two or more images into a single compound

Fig .4 Splicing

2) **Cloning (Copy-Move)**

Image exploitation method of replicating or copying one part of the image directly into another part of the image.

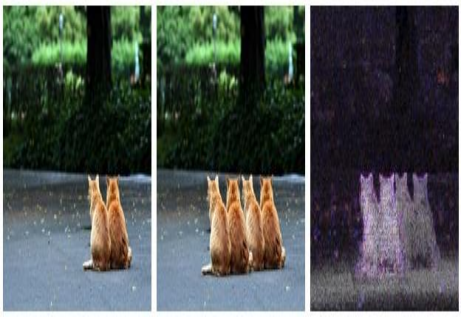

Fig. 5 Cloning

There are three categories are:

1. Low Level. Statistical characteristics of digital image pixels or DCT coefficients used by low level methods Using a model of authentic images which tampered images do not satisfy for forgery detection also belongs to this level.
2. Middle Level. At this level, we detect the trace of forgery operation which has some simple semantic information, like splicing1 caused sharp edges, inconsistencies of lighting direction, etc.
3. High Level. i.e.,semantic level. Actually, it is very hard for computer to use semantic information to do forgery Detection because the aim of forgery is changing the meaning of image content it originally conveyed.

3**. Image Re-touching***:*

Image Retouching is considered as less harmful kind of digital image forgery than other types present. In case of image retouching original image does not significantly changes, but there is enhancement or reduces certain feature of original image. This technique is popular among magazine photo editors. This type of Image forgery is present in almost all-magazine cover that would employ this technique to improve certain features of an image so that it is more attractive.[6]

IV. Tools Of Image Forensic

The set of image forensic tools are categorized into five categories:
1) pixel-based techniquesthat detect statistical anomalies introduced at the pixel level;
2) format-based techniquesthat influence the statistical correlations introduced by a specific lossy compression scheme;
3) camera-based techniquesthat use artifacts introduced by the camera lens, sensor, or on-chip post processing;
4) Physically based techniquesthat explicitly model and detect anomalies in the three-dimensional relations between physical objects, light, and the camera; and
5) geometric-based techniquesthat make measurements of objects in the world and their positions relative to the camera.[10]

V. Applications Of Image Tampering

Tampering is normally done to cover objects in an image in order to either produce false proof or to make the image more pleasant for appearance.
1. In the field of medicine, reports of patients are highly confidential and are always supposed to be authentic. Medical images are produced in most of the cases as proof for unhealthiness and claim of disease. Also medical results are usually placed as proofs or alternatives for avoiding punishments in courts.So thesetype of tampering with medical images disturbs the security of the mutual individual.
2. In the field of education, different tampering techniques give us false information which in turns leads to the delivery of incorrect data to the organization. Students carried out large amount of forgery with their documents for their own benefit. This disturbs the security of the management which is an urgent issue to be solved.
3. In the field of agriculture, tampering is also done with the different images used during the training of the farmers which results to the misguidance to the agricultural students. This type of forgery imbalance the security management which is to be solve soon.
4. In the field of e-commerce, most of the transactions are carried out through internet whether it is money transfer, Shopping purpose, bill payment etc. In this, Security of the customer's details is the prime focus of the government. But many unauthorized users manipulate the data which results in serious crime. Tampering is a major risk to the technology which requires immediate attention.[11]

VI. Litreture Survey

Surbhi gupta, [1] This paper aims at detecting image manipulations by exploiting the discrepancies which arise due to image quality decline. RGB, YCbCr and L*a*b color model are used to check the quality deterioration. Characteristics based features are extracted and then utilized for differentiating original image from manipulated one.

Saurabh Agarwal et.al, [2] In this paper, Image tampering detection is important due to many incidences of tampered images misuse. we propose a hybrid approach for image tampering detection using range filter and quality descriptor. First we highlights importantdetails of the image using range filtering. The range filter highlights the edges, contours andimportant details ofthe objects in an image. Further we apply texture descriptor based on local phase of the image in frequency domain is applied to extract crucial features of the image.

Musaed Alhussein, [3]A new image tampering detection method based on local texture descriptor and extreme learning machine (ELM) is proposed in this paper. The image tampering includes both splicing and copy-move forgery. First, the image was divided into three color channels (one luminance and two Chroma), and each channel was divided into non-overlapping blocks. Local textures in the form of local binary pattern (LBP) were take out from each block. The histograms of the patterns of all the blocks were concatenated to form a feature vector.

David Asatryan et.al,[4] In this paper, a watermarking algorithm is used, which allows handling over the images at different ratios of sizes of image-container and watermark. Most of the types of image tampering are based on the well known operations of Copy-Paste, Copy-Move or their combinations. In many investigations the basic approach for tamper detection is based on creating a watermarking procedure in such a way that the type and parameters of distortion of the watermark from an attack allow to make an inference on the presence of a fraud, to locate the damaged parts of the image and even to recover them..

Snigdha K. Mankar, [5] In this paper, presents a review of Image forgery technique. There are two types of techniques for image forensics: one is active protection, and the second one is passive detection. The main types of Image forgery techniques are Image Splicing, Copy-Move forgery. Now a days the forgery of Images is increasing ,it is very much necessary to develop tools for detection as which image is true and which is forgery. In this paper, we study on of the most powerful technique like the SVM classifier, Pixel-based and partition-based to detect forgery images.

Swati A.Khavare, [6] In this Paper, proposes the novel technique for Active tamper detection and tamper localization, which uses image hashing algorithm applied on extended imagebased onring partition and Non Negative Matrix Factorization (NMF). Key contribution is tamperdetection in small region especially corner regions and exact localization of that tampered object. Particular tampered region is localizedwith the help of recursive use ofimage hashing algorithm on each division of image in significantly less time.

Nishtha Parashar et.al, [7] Due to powerful computers and advanced photo-editing software tools the manipulation of images has become an easy task. Confirming the authenticity of images and detecting tampered regions in an image without any knowledge about the image content is an important part of the research field. An effort is made to survey the recent advancements being made in the field of digital image forgery detection and thus passive methods for forgery detection are being presented. Blind or passive methods do not require any precise former information about the image. In the first part, various image forgery detection techniques are characterized and then an overview of passive image authentication is presented and the existing blind forgery detection techniques are reviewed.

Vinayak S. Dhole,[8]This paper introduces a modified fragile watermarking technique for image recovery. Here we can detect as well as recovered the tampered image with its tampered region. Birthday attack, college attack and quantization attacks are modified approach which helps us to produce resistance on various attacks. Using a non-sequential block chaining and randomized block chaining, which is created on the basis of secrete key this modified technique produces great amount of recovery from tampered regions. In this modified technique we put a watermark information.

Nirupama, et.al, [9] In this paper, we focus on image forensic detection on tampered pictures. The detection of a tampering in image is driven to provide authenticity and to maintain integrity of the image so that tampering is detected and minimized.

VII. Conclusion

In this paper, a brief survey of Digital image forgery classification and its detection methods have been presented. An attempt is made to bring in various potential algorithms that signify improvement in image authentication techniques. The techniques discussed above are useful for detecting cut and paste type forgeries. Thus extensive survey is done in this paper to detect duplication in images and provides future enhancement directions in the area of image forgery detection.

References

[1]. Surbhi gupta**,**"Highlighting Image Tampering by feature Extraction based on Image Quality Deterioration",2016 International Conference on Computing for Sustainable Global Development (INDIACom),978-9-3805-4421-2/16/$31.00_c 2016 IEEE

[2]. Saurabh Agarwal1 and Satish Chand2,"Image Tampering Detection using Local Phase based Operator", International Conference on Emerging Trends in Electrical, Electronics and Sustainable Energy Systems (ICETEESES–16),978-1-5090-2118-5/16/$31.00 ©2016 IEEE

[3]. Musaed Alhussein, "Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine", 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, 978-1-5090-0888-9/16 $31.00 © 2016 IEEE DOI 10.1109/UKSim.2016.39

[4]. David Asatryan#, Naira Asatryan*, Natalya Lanina*, Alexander Petrosyan*, "Method for Detection of Image Tampering and Partial Recovery", unpublished.

[5]. Wei Wang, Jing Dong, and Tieniu Tan, "A Survey of Passive Image Tampering Detection". Springer-Verlag Berlin Heidelberg 2009

[6]. Snigdha K. Mankar, "Image Forgery Types and Their Detection", Volume 5, Issue 4, April 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering,© 2015, IJARCSSE.

[7]. Swati A.Khavare, "Robust Image Hashing Algorithm for Detecting and Localizing Image Tamper in Small Region", 2015 International Conference on Information Processing (ICIP)Vishwakarma Institute of Technology. Dec 16-19, 2015,978-1-4673-7758-4/15/$31.00 ©2015 IEEE.

[8]. Nishtha Parashar1 and NirupamaTiwari2, "A Survey Of Digital Image Tampering Techniques", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.10 (2015), pp.91-96,ISSN: 2005-4254 IJSIP

[9]. Vinayak S. Dhole, "Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks", 2015 International Conference on Computing Communication Control and Automation,978-1-4799-6892-3/15 $31.00 © 2015 IEEE.

[10]. Nirupama Tiwari[1], Deepika Dubey[2] , Anshi Goyal[3], "Reducing Forged Features Using Tampered andInconsistent Image Detection Techniques In Digital Image Processing", 2015 Fifth International Conference on Communication Systems and Network Technologies,978-1-4799-1797-6/15 $31.00 © 2015 IEEE

[11]. Deepika Sharma and Pawanesh Abrol," Digital Image Tampering – A Threat to Security Management", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013