Chavi Rana, 2021, 9:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Digital Image Forgery Techniques and its Detection

Research Scholar Chavi Rana, Asst. Prof. Gyanendra Kumar Singh
Dept. of Computer Science
Sunder Deep Group of Institutions,
Ghaziabad,UP,India

Abstract- The billions of digital images flooding the internet which are widely used and regards as the major information source in many fields in recent years with the high advance of technology, it may seem easy to fraud the image. In digital images, copy-move forgery is the most common image tampering, where some object(s) or region(s) duplicate in the digital image. The important research has attracted more attention in digital forensic is forgery detection and localization. Many techniques have been proposed and many papers have been published to detect image forgery. This paper introduced a review of research papers on copy-move image forgery published in reputed journals and focused on discussing various strategies related with fraud images to highlight on the latest tools used in the detection. This article will help the researchers to understand the current algorithms and techniques in this field and ultimately develop new and more efficient algorithms of detection copy-move image.

Keywords: Copy –Move Detection, JPEG Image Morphing, Copy Paste, DWT.

I. INTRODUCTION

Various researchers have proposed different algorithms for finding the most sensitive areas. When looking at the false regions, few algorithms are effective, but it is time consuming. Some algorithms may not be able to detect fraud, but it takes less time to kill. However, very few algorithms can detect forgetting with less execution time, but they are less resistant to various attacks (such as rotation, scaling, explosion, multiple scratches, and pinching etc.) Search for digital surveillance cameras is divided into active and passive technologies.

In advanced technology, digital picture verbs require image processing, that is, signatures and water extraction, which limit their applicability or applicability to the system. Based on the opposite, water extraction and signature technology; Pacific technology does not need to generate digital media or pump water. In addition, the pacifist methods for detecting image forgetting are divided into five types, as shown in Figure 1. In addition, pixel-based methods mainly identify statistical averages applied to pixel height. On the other hand, the calculation method controls the statistical correction used by the specific lens tracking system, in addition, the camera capture method was used by the artifact introduced by the camera or sensor level and in production.

In terms of the physical environment, we model it clearly and notice the rarity of the three-way interaction between physical objects and light and the camera. Finally, the geometrical method determines the size of the universe and its position relative to the camera.

Pixel-based technology mainly focuses on detecting image anomalies that have been included in the forgetting process. These are the most popular techniques for forensic photography, which are also divided into three categories, namely cloning (copying and mobilization), discipline and editing. Publishing-based technology depends on the form and format of JPEG. The technology is divided into three categories, namely, JPEG, double JPEG and JPEG.

The camera-based approach focuses on identifying the specifications by using the artifacts applied at various stages of the image processing. It is also divided into four categories, namely chromatic aberration, color sensor, camera response and sensor sound.

Basic physical technology depends on the calculation of the light and the inconsistency of the light between the areas of the image, as a distinctive feature in image processing, which is also divided into three types, is a 2D light path, a 3D light path and a lightweight environment.

Geometric techniques depend on the calculation of the major points moving to the image area and the differences between the main points. The technique is another of two categories, namely the main point and the meter measurement. Image editing is the most common way of creating an image, where a child or a specific image object is combined and then sent to another location with similar images to fill in all the information.

When a given block is created with a similar image, its textual features (that is, the soundboard and color palette) will be the same as the rest of the image, so every time we want to see and see, Various methods have been developed for the recovery of cloning activity of image examinations, and these methods depend on the pairing technique or the key matching technique.

1. Image Retouching:

Enhancement in an image by adjusting contrast, brightness, noise level and also by edge sharpening and smoothing. In this forgery, the sole motive is to provide an image with better visualization.

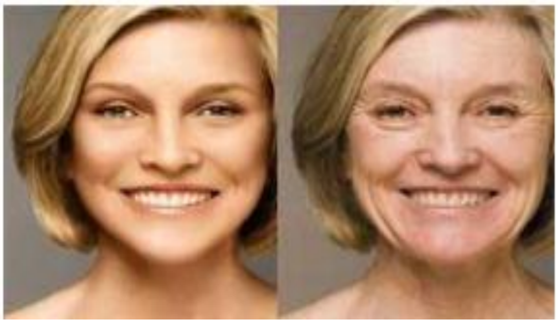

Fig 1. Image Retouching.

2. Image Splicing:

Original image combined with two or more different images to make a forged image. In this regions from different images are taken to change original image. To identify such kind of forgery the focus is on identifying incompatibilities in image characteristics as regions of different images are used for making forged image.

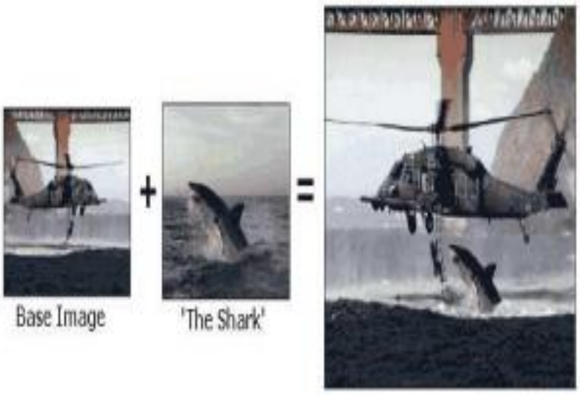

Fig 2. Image Splicing.

3. Discrete Wavelet Transform:

A wavelet function is a small wave that concentrates its energy over time. It is used to analyze in terms of time and frequency stationary, non-stationary and time-variable phenomena. The wavelet transform is considered to be the most powerful form of signal representation that can be applied mainly to the processing of signals and images.

There are numerous types of wavelet families, the most important are: Haar, Daubechies, Biorthogonal, Coiflets, Symlets, and Morlet, Mexican Hat, Meyer, Reverse Biorthogonal, Frequency B-Spline, and Gaussian derivatives.

The discrete wavelet transform (DWT) can provide unique and discriminating representations that can quantify vital and interesting structures such as edges and details with good resolution for few coefficients. It is also computationally effective due to the small amount of data with which it works.

The final wavelet coefficients can be used directly as characteristics and can be extracted directly from the wavelet domain, describing the anomalies in the image data. Basically, the discrete wavelet transform reduces the correlation between wave coefficients and provides energy compaction in some wavelet coefficients.

II. IMAGE FORGERY

The semantic information of an image is altered by addition or extracting information from the image. In order to achieve the image forging, numerous ways are used by the forgers.

In general, there exist different types of the image forgery. The categorization of the types of image forgery is a tedious task; this is because the forgery types are grouped based on the process involved creating the fake image. But in the current technical world, new innovations are made in the digital photography, which ascend new malicious forging techniques day by day.

However, based on the existing types, a categorization is made in this research explaining different types of the image forgery [5] Figure 1 depicts the different types of image forgery. Image Retouching-Image retouching is one of the less harmful digital image forgery techniques. It is said so because it doesn't alter the visual messages of an image Al-Hammadi M. Image editing is the main mechanism in image retouching.

In this method, the images are edited with different background, attractive colors, and work with the hue saturation for toning and balancing the image is performed. It is used to enhance the image quality to capture the reader's attention.

Now a day, the image retouching forgery is familiar in social media like Face book, Twitter etc., where the users post their retouched image by addition of filtering, etc. to acquire more favorites (likes) for the image.

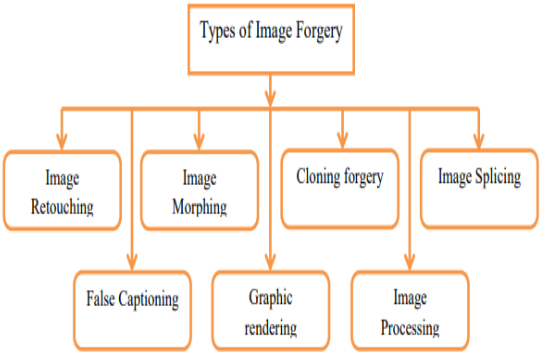

Fig 3. Types of image forgery.

1. Image Morphing:

Image morphing is a different type of forgery. In this method, the original image is transformed into another image by smooth transition of images .An example for morphing is available in xmorph.sourceforge.net. The image forging type forgery is critical nowadays leading to scandals.

2. Copy Paste:

Copy paste forgery is considered to be the most common type of the image forgery. In this method, the regions from the original images are copied and pasted within the same image.

In certain cases; the images are pasted within with possible transformation. The region duplication is the main intend of the copy paste forgery. The copy paste forgery is also called a copy move forgery or region duplication forgery or cloning. The copy move forgery is realized into different types based on the way on which the duplicated region is pasted in the original image.

They are

- Copy move with rotation
- Copy move with a different scale
- Copy move with reflection etc.

3. Active Forgery identification Techniques:

An active forgery detection technique requires pre-extracted or pre-embedded information. Digital Watermarking or digital signatures are popularly known methods used in Active approach.

4. A passive Forgery detection Techniques:

Passive method, popularly known as blind methods, merely uses the image itself for its authentication and integrity. This method assumes that although there may be no visual clues of tampering in the image, but tampering may disturbs the underlying statistics property due to the Noise inconsistency, Blurring of image, Image sharpening, Forgery through copy-move and Image in painting etc.

Forgery dependent techniques are intended to distinguish just certain kind of forgeries, like splicing those are reliant on the sort of forgery carried out on the picture [9]. Forgery independent techniques recognize forgeries that are independent from fraud but in view of artifact traces left behind due to the procedure of sharpening, blurring and because of inconsistencies due to shading and light effects.

5. Generalized Schema For Image Forgery Identification:

Forgery identification in pictures is two step issues. The principle target of blind forgery detection technique stays to categorize a given picture as real or altered. [10]

We will depict a widely used schema of image forgery identification procedure that comprises of the following steps:

5.1 Image Preprocessing: Image preprocessing is the initial pace. Some preprocessing is performed on the picture under deliberation like image filtering, image enrichment, trimming, change in DCT coefficients, RGB to grayscale transformation before handling the image to feature extraction procedures. Algorithms examined at this juncture might possibly include this step depending upon the calculation

5.2 Feature Extraction: Selection of features for every class separates the image-set from different classes however in the meantime stays constant intended for a specific class chosen. The attractive element of the chosen set of features is to have a tiny measurement so that computational complexity can be diminished and have an extensive distinction with other classes

5.3 Selection of Classifier: Depending upon the feature-set that is extracted in above step, suitable classifier is either chosen or composed. The large training sets will yield the improved performance of classifier

5.4 Classification: The only motive behind classification is to determine if the image is original or not.

5.5 Post Processing: Some forgeries will possibly require post processing that includes manipulations like localization of copy locales.

III. LITERATURE REVIEW

Various researchers have proposed different algorithms for finding the most sensitive areas. When looking at the false regions, few algorithms are effective, but it is time consuming. Some algorithms may not be able to detect fraud, but it takes less time to kill. However, very few algorithms can detect forgetting with less execution time, but they are less resistant to various attacks (such as rotation, scaling, explosion, multiple scratches, and pinching, etc.) Search for digital surveillance cameras is divided into active and passive technologies. In advanced technology, digital picture verbs require image processing, that is, signatures and water extraction, which limit their applicability or applicability to the system. Based on the opposite, water extraction and signature technology; Pacific technology does not need to generate digital media or pump water. In addition, pixel-based methods mainly identify statistical averages applied to pixel height.

On the other hand, the calculation method controls the statistical correction used by the specific lens tracking system, in addition, the camera capture method was used by the artifact introduced by the camera or sensor level and in production. In terms of the physical environment, we model it clearly and notice the rarity of the three-way interaction between physical objects and light and the camera. Finally, the geometrical method determines the size of the universe and its position relative to the camera.

1. Pixel-Based Technology:

In this technology mainly focuses on detecting image anomalies that have been included in the forgetting process. These are the most popular techniques for forensic photography, which are also divided into three categories, namely cloning (copying and mobilization), discipline and editing.

2. Publishing-Based Technology:

This technology depends on the form and format of JPEG. The technology is divided into three categories, namely, JPEG, double JPEG and JPEG.

3. The Camera-Based Approach:

This technology focuses on identifying the specifications by using the artifacts applied at various stages of the image processing. It is also divided into four categories, namely chromatic aberration, color sensor, camera response and sensor sound.

4. Basic Physical Technology:

This technology depends on the calculation of the light and the inconsistency of the light between the areas of the image, as a distinctive feature in image processing, which is also divided into three types , is a 2D light path, a 3D light path and a lightweight environment.

5. Geometric Techniques:

These technologies depend on the calculation of the major points moving to the image area and the differences between the main points. The technique is another of two categories, namely the main point and the meter measurement. Image editing is the most common way of creating an image, where a child or a specific image object is combined and then sent to another location with similar images to fill in all the information.

When a given block is created with a similar image, its textual features (that is, the soundboard and color palette) will be the same as the rest of the image, so every time we want to see and see, it will cause a huge loss, Threats. Various methods have been developed for the recovery of cloning activity of image examinations, and these methods depend on the pairing technique or the key matching technique.

Amanpreet Kaur et. al (2018) Mobile forgetting is the most common form of forgetting. For monitoring the writing process, a wall-based approach and a key point-based approach can be used. I, key point-based features are selected because the difficulty of following them is lower than that of block-based features. The four different optimization algorithms based on the main points, namely, SURF, KAZE, Harris corner and BRISK, are estimated to test their effectiveness in tracking copying events.

The methodology consists of four steps: image preparation, interesting detector, vector description and feature mixing. The results are compared to the true, the number fl, and the accuracy, which is calculated using a single strategy in the matching algorithm. It can be concluded that in all practical directions the KAZE function can provide the best results, and since the Harris corner is not aligned and the corners are detected instead of the corner, the Harris corner is not suitable for operation Fake.

Navdeep Kanwal et al. (2019) Media protection is one of the major challenges facing the world today, given the growing reliance on multimedia information. Easy-to-use image editing software allows all users of mobile phones and computers to attack image and video information and make changes to some extent. To verify the authenticity of the image, it takes time to identify the image processing. a variety of skills have been proposed to use features to determine image forgetting. Creation control technology plays a role in both areas of image forgetting.

This article provides a comprehensive analysis of image test results by defining local text (LBP) and local ternary mode (LTP)). This paper proposes a technique for integrating (FFT) with localized text for picture capture detection using block-based methods.

The influence of technology and descriptors has been tested against the CASIA v1.0 benchmark. We evaluate the results by using standard test methods to test accuracy and recall rates. The paper also offered a more attractive version.

Taranjit Kaur et.al (2018) the present age is digital photography, and we believe that the form of photography has evolved. Creating a search engine is a technique for detecting clones in images. Because of the variety of images, the editing tools make it easy for users to manipulate images and create digital images of them. Forgetting recovery has a variety of technologies, such as active technology and passive technology.

In addition, attributes such as analysis and classification are used to identify forgeries. The work described in this article is based on the emphasis on forgetting about forgetfulness. Cloning memory technology is a type of memory cloning technology. In memory cloning technology, some parts of the image are copied and transferred to other parts of the image, which are not easily visible to the naked eye.

PCA (Principle Component Analysis) technology is used to find different space from an image. In its proposal, the GLCM (Gray Scale Co-emergence Matrix) technology is used in conjunction with PCA for false deception. The proposed work is performed at MATLAB, and depends on the PSNR, the rate of recall, its performance, and its accuracy.

In his proposal, the result is better than the failure rate or the recovery from two different attacks (Gaussian noise and landfill). Studies show that compared to existing algorithms, the algorithms is good. In the existing method, the results of the definitions such as accuracy are incorrect in the proposed method. In addition, the proposed method achieves earlier memory and higher memory.

Ali Mumcu et al. (2018) due to the frequent use of built-in image processing tools, it is easy to manipulate digital images. Mobile forgetting is one of the most often forgotten techniques for simple simplicity. In the literature, the removal of this type of invention is divided into two parts: fixed and key point based. This paper presents fraudulent views based on key points. This work uses the main points derived from the FAST algorithm and the calculation vector calculation of the SIFT algorithm. In addition, parallel programming techniques are used to reduce program flow during the implementation of this method.

H.M. Shahriar Parvez et al. (2018) currently, the popularity of basic visual media applications is increasing when information is available. The rapid development of technology has led to improved image processing tools and easier image forgetting. As a result, it becomes a difficult issue in the later stages. In this case, checking the legitimacy and validity of digital images will become a major issue. Forgetting the hardest part is translating portions of images and uploading them to different areas of the same image.

This study proposes an effective approach to regional regression. This study is divided into recurrent distributions based on the regression analysis method. Creating algorithms based on image sharing, Gabor decoding and K-Means modeling. Initially, the image was distributed via high quality custom recognition technology (NCut). Then, the Gabor filter is used to capture the image, and the same feature is closed using K-Means clustering. Finally, comparing the control area to a given one determines the authenticity of the image.

Umair A. Khan et. al (2018) since technology has evolved to the point where many free software is used to change the image content, the accuracy of digital photography is guaranteed. This poses particular challenges in determining the validity of digital images, particularly when it is obtainable as legal proof.

Many methods have been proposed to determine image memory, although the success of each depends on the type of memory and / or features used to detect the memory. Therefore, their specific actions in terms of accuracy and execution time are different. This article focuses on the most common image test, called mobile memory. There are two aspects to the work in this article. First, the hybrid approach is proposed, which combines box-based and non-furniture-based technologies to test innovation initiatives. Second, various features of the images are used to evaluate the technological capabilities presented.

Assessment criteria that include accuracy, accuracy, recall, F-1 score and execution time help to determine the tradeoff required between correctness and implementation time.

The results presented in this paper show that the image-based surveillance technology offered is capable of detecting duplication of correct copywriting events and possible execution times. In addition, the proposed technique works well with colorful and colorful images as well.

Gül Muzaffer et al. (2018) In recent years, with the advancement of technology, various topics such as public, medical, military and forensic have become digital. The bad guys can upload digital images mentioned almost every scene using image editing software. The most common way of forgetting images is to translate and manipulate forgetting. In this work, a line-based approach is proposed to identify event forgetting.

Images taken from the block using Local Density Line Mode (LIOP) are a newer and more effective method, which is integrated with the Patch Match algorithm to quickly detect forgetting of copying events. In addition, these were compared to recent works and tested against resistance. Experimental results show that although the riot is audio, jumble, rotation, deception and JPEG scaling, the algorithm can detect forgetting of a recording event.

Khushkaran Kaur et.al (2018) today, it's very easy to manipulate digital images in a smart way. As image processing systems develop rapidly, the use of these strategies is also increasing. As a result of exploiting these systems, image stabilization has become a very difficult task. Copy-and-paste copying is the most widely accepted method of image editing, where some parts of the image are copied and pasted into other parts of the same image to hide or copy certain parts of the image. Therefore, police and specialists need production methods for repeated production. In this paper, a methodology is used to identify the write memory activity. First, the generated images are divided into overlapping barriers, and then KPCA (Kernel Principal Component Analysis) is used to remove the features, and then combine these patterns.

By defining the corresponding bars in the image, a series of generated images can be found. Experimental results show that although the translation has changed the image (including limited angel rotation, reduced shadow, and shifts in brightness), the planned tactic may see the translated location. Compared to traditional gradient histogram (HOG) techniques, this method improves accuracy, accuracy and specificity, and reduces the level of error detection and time required to find out how to make a fake copy. Get good results.

B Chaitra et al. (2019) with the significant development of digital image processing software tools and their propaganda has enabled users to easily manipulate and convert digital images.

Digital photography sometimes establishes essential principles and creates useful evidence in various fields such as forensic investigations, criminal investigations and legal investigations, medical imaging, and news. It raises questions about the origin, legality and security of digital photography. This article first introduced new image processing technologies, tools for writing, and discussed strategies for introducing various image processing technologies.

Gul Muzaffer et. al (2019) Because the image processing program is so easy to use, forgetting the action is the simplest way to change the image, which aims to copy or delete the objects in the image. How to fix this fake product is divided into: a key point-based, user-friendly method that uses manual operation.

There is a new forgetfulness tracking strategy based on deep learning. Alex Net's existing training model is used to break down the image vectors by fully rotating the image. After the feature was acquired, the similarities between the feature vectors were learned to find and construct the memory. As reported by the results obtained, this method has a higher degree of caution than traditional methods considered in the literature.

IV. CONCLUSION

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, 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 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] Amanpreet Kaur, Savita Walia, Krishan Kumar, Comparative Analysis of Different Key point Based Copy-Move Forgery Detection Methods 2018 Eleventh International Conference on Contemporary Computing (IC3) Year: 2018 ISBN: 978-1-5386-6835-1 DOI: 10.1109/IEEE Noida, India.

[2] Navdeep Kanwal, Akshay Girdhar, Lakhwinder Kaur, Jaskaran Singh Bhullar, Detection of Digital Image Forgery using Fast Fourier Transform and Local Features 2019 International Conference on Automation, Computational and Technology Management (ICACTM)Year: 2019 ISBN: 978-1-5386-8010-0 DOI: 10.1109/IEEE London, United Kingdom.

[3] Taranjit Kaur, Akshay Gerhard, Geetika Gupta, A Robust Algorithm for the Detection of Cloning Forgery 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) Year: 2018 978-1-5386-1508-9 DOI: 10.1109/ IEEE Madurai, India.

[4] Ali Mumcu Ibrahim Savran Copy move forgery detection with using FAST key points and SIFT description vectors 2018 26th Signal Processing and Communications Applications Conference (SIU) Year: 2018 ISBN: 978-1-5386-1501-0 DOI: 10.1109/IEEE Izmir, Turkey.

[5] H.M. Shahriar Parvez Hamid A. Jalab Ala'a R. Al-Shamasneh Somayeh Sadeghi Diaa M. Uliyan

Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)Year: 2018 ISBN: 978-1-5386-4838-4 DOI: 10.1109/IEEE Shah Alam, Malaysia.

[6] Umair A. Khan Mumtaz A. Kaloi Zuhaib A. Shaikh Adnan A. Arain A Hybrid Technique for Copy-Move Image Forgery Detection 2018 3rd International Conference on Computer and Communication Systems (ICCCS) Year: 2018 ISBN: 978-1-5386-6350-9 DOI: 10.1109/ IEEE Nagoya, Japan.

[7] Gül Muzaffer Eda Sena ErdölGüzin UlutaşA copy-move forgery detection approach based on local intensity order pattern and patchmatch2018 26th Signal Processing and Communications Applications Conference (SIU) Year: 2018 ISBN: 978-1-5386-1501-0 DOI: 10.1109/ IEEE Izmir, Turkey

[8] Khushkaran Kaur Efficient and Fast Copy Move Image Forgery Detection Technique 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) Year: 2018 ISBN: 978-1-5386-2842-3 DOI: 10.1109/ IEEE Madurai, India.

[9] B Chaitra P.V Bhaskar Reddy A Study on Digital Image Forgery Techniques and its Detection 2019 International Conference on contemporary Computing and Informatics (IC3I Year: 2019 ISBN: 978-1-7281-5529-6 DOI: 10.1109/ IEEE Singapore, Singapore.

[10] Gul Muzaffer Guzin Ulutas A new deep learning-based method to detection of copy-move forgery in digital images 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT) Year: 2019 ISBN: 978-1-7281-1013-4 DOI: 10.1109/ IEEE Istanbul, Turkey.