Shailja Mansingh Choudhary, 2021, 9:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Review on Digital Image Copy – Move Detection

Shailja Mansingh Choudhary
M.Tech. Scholar
Branch: [EC] Digital Communication
Truba Institute of Engg. &amp
Information Technology
shailja.choudhary15@gmail.com

Abhishek Agwekar
Head of Department
Branch: Electronics and Communication
Truba Institute of Engg. &amp
Information Technology
abhishek.agwekar@trubainstitute.ac.in

Abstract- Digital images are used everywhere and it is easy to manipulate and edit because of availability of various image processing and editing software. In a copy-move image forgery, a part of an image is copied and then pasted on a different location within the same image. A copy-move image forgery is done either for hiding some image object, or adding more details resulting in at least some part being cloned. In both the case, image reliability is lost. In this paper an improved algorithm based on Discrete Wavelet Transform (DWT) is used to detect such cloning forgery. In this technique at first DWT (Discrete Wavelet Transform) is applied to the input image for a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. After that Lexicographic sorting is performed, and duplicated blocks are identified. Due to DWT usage, detection is first carried out on lowest level image representation. This approach increases accuracy of detection process and reduces the time needed for the detection process.

Keywords:- Copy-Move forgery, Digital Tempering, DWT, Cloning.

I. INTRODUCTION

Because of different types of digital cameras and user-friendly image editing software people can create and manipulate digital images easily. A digitally changed photograph can be indistinguishable from an authentic photograph. As a result, photographs no longer hold the unique stature as recording of events.

Copy-Move forgery is performed with the intention to make an object "disappear" from the image by covering it with a small block copied from another part of the same image because the copied parts come from the same image, noise components, Brightness, the color palette, and the other properties will be well-matched with the rest of the image, therefore it is very difficult for a human eye to detect such forgery.[1]

Since the key characteristics of Copy-Move forgery is that the copied part and the pasted part are in the and more time is needed for detection. Therefore to increase the speed of operation process many researchers use blocking approaches. D. Soukal, proposes DCT based copy-move forgery detection in a single image, In which The image blocks are represented by quantized DCT (Discrete Cosine Transform) coefficients, and a lexicographic sort is adopted to detect the duplicated image blocks.

A. C. Popescu and H. Farid proposed a similar detection method [4], in which the image blocks are reduced in dimension by using Principal Component Analysis (PCA). But the efficiency of detection algorithm was not good, because, blocks are directly extracted from the original image, resulting in a large number of blocks, G.Li, Q.Wu, D.Tu developed a sorted neighborhood method based on DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition).

In this method the computation of SVD takes lot of time and it is computationally complex. B. L. Shiva

kumar and Dr. S.Santhosh Baboo have proposed copy-move forgery detection method based on SURF, which detects duplication region with different size. Experimental result shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution.[2]

To further reduce the amount of computation, this paper proposes wavelet based approach where the use of wavelet transform reduces the dimensional representation of tampered images and shift vector is used as similarity checking criterion for identifying duplicity of overlapping blocks formed from the tampered images.

(a) (b)

Fig 1. Example of Copy-Move forgery (a) original image (b) tampered image.

Forgeries are not new to mankind but are a very old problem. In the past it was limited to art and literature but did not affect the general public. Nowadays, due to the advancement of digital image processing soft-ware and editing tools, an image can be easily manipulated and modified. It is very difficult for humans to identify visually whether the image is original or manipulated. There is rapid increase in digitally manipulated forgeries in mainstream media and on the Internet [3].

This trend indicates serious vulnerabilities' and decreases the credibility of digital images. Therefore, developing techniques to verify the integrity and authenticity of the digital images is very important, especially considering that the images are presented as evidence in a court of law, as news items, as a part of medical records, or as financial documents. In this sense, image forgery detection is one of the primary goal of image forensics [4].

II. TYPES OF DIGITAL IMAGE FORGERY

Picture altering is characterized as "adding, changing, or deleting some important features from an image without leaving any obvious trace [5]. There have been different techniques utilized for forging an image. Taking into account the methods used to make forged images, digital image forgery can be isolated into three primary classifications: Copy-Move forgery, Image splicing, and Image resampling.

1. Copy-Move Forgery:

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 in Figure 1. As the copied part originated from the same image, its essential properties such as noise, color and texture don't change and make the recognition process troublesome.

2. Image Forgery using Splicing:

Image splicing uses cut-and-paste systems from one or more images to create another fake image. When splicing is per-formed precisely, the borders between the spliced regions can visually be imperceptible. Splicing, however, disturbs the high order Fourier statistics. These insights can therefore be utilized as a part of distinguishing phony. Figure 2, demonstrates a decent sample of image splicing in which the pictures of the shark and the helicopter are merged into one picture.

Fig 2. (a) The real image (b)Result of image retouching.

3. Image Re-sampling:

To make an astounding forged image, some selected regions have to undergo geometric transformations

like rotation, scaling, stretching, skewing, flipping and so forth. The interpolation step plays a important role in the resampling process and introduces non-negligible statistical changes. Resampling introduces specific periodic correlations into the image. These correlations can be utilized to recognize phony brought about by resampling. In Figure 3, the picture on the left is the original image while the one on the right is the forged image obtained by rotation and scaling it.

III. DIGITAL IMAGE FORGERY DETECTION METHODS

Digital image forgery detection techniques are grouped into two categories such as active approach and passive approach. In the active approach, certain information is embedded inside an image during the creation in form of digital watermark.

Drawback of this approach is that a watermark must be inserted at the time of recording, which would limit to specially equip digital cameras. In the passive approach, there is no pre-embedded information inside an image during the creation. This method works purely by analyzing the binary information of an image. Passive image forgery detection techniques roughly grouped into five categories [6].

1. Pixel-Based Image Forgery Detection:
Pixel-based techniques accentuate on the pixels of the digital image. These techniques are generally classified into four sorts such as copy-move, splicing, resampling 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.

2. Format-Based Image Forgery Detection:
Format based techniques are another kind of image forgery detection techniques. These are mainly based on image for-mats, in which JPEG format is preferable. Statistical correlation introduced by specific lossy compression schemes, which is helpful for image forgery detection.

These techniques can be partitioned into three sorts such as JPEG quantization, Double JPEG and JPEG blocking. If the image is compressed then it is exceptionally hard to identify fraud however these techniques can detect forgery in the compressed image.

3. Camera-Based Image Forgery Detection:
Whenever we take a picture from a digital camera, the picture moves from the camera sensor to the memory and it experiences a progression of processing steps, including quantization, color correlation, gamma correction, white adjusting, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may shift on the premise of camera model and camera antiques.

These techniques work on this standard. These methods can be separated into four classes such as chromatic aberration, color filter array, camera response and sensor noise.

4. Physical Environment-Based Image Forgery Detection:
These techniques basically based on three dimensional interactions between physical object, light and the camera. Consider the creation of a forgery showing two movie stars, rumored to be romantically involved, strolling down a nightfall shoreline. Such a picture may be made by grafting together individual pictures of each movie star. In this manner, it is frequently hard to exactly match the lighting effects under which each individual was initially captured.

Contrasts in lighting across an image can be utilized as proof of altering. These techniques work on the basis of the lighting environment under which an article or picture is caught. Lighting is very important factor for capturing an image. These techniques are isolated into three classifications such as light direction (2-D), light direction (3-D) and light environment.

5. Geometry-Based Image Forgery Detection:
These techniques basically based on principal point i.e. projection of the camera center onto the image plane, that make measurement of the object in the world and their position relative to camera. Grooves made in firearm barrels confer a twist onto the shot for increased accuracy and range. These grooves acquaint to some degree particular markings to the bullet fired, and can consequently be utilized with a particular handgun.

In the same soul, several image forensic techniques have been produced that particularly display relics presented by different phases of the imaging procedure. Geometry-based image forgery detection methods are serrated into two classes such as principle point and metric measurement.

IV. LITERATURE REVIEW

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. [7]

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.[8]

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.[9]

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 are 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.[10]

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.[11]

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. [12]

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.[13]

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.[14]

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.[15]

V. DWT TRANSFORM

Step 1. The Discrete Wavelet Transform is basically used to reduce the size of the image at each level, e.g., a square image of size 2 i ×2i pixels at level L reduces to size 2 i/2 × 2i/2 pixels at next level L+1.The image is decomposed into four sub images, at each level. The sub images are labeled LL,LH, HL and HH[7]. LL corresponds to the coarse level coefficients or the approximation image. This image is used for further decomposition.

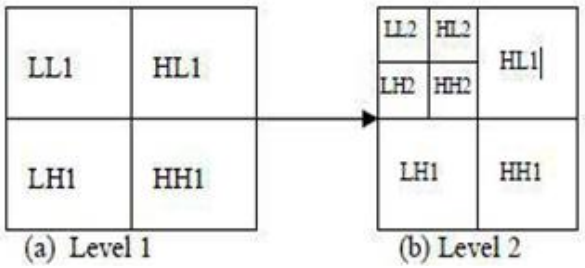

Fig 3. (a) level-1 dwt (b) level-2 dwt.

Step 2. After that a B×B block is sided over the resulting image e and image is scanned from the upper left corner to the lower right corner. The DWT transform is calculated, For each block, the DWT coefficients are stored as one row in the matrix A. The matrix will have (M-B+1)×(N–B+1) rows and B×B columns, Where M and N represents number of rows and columns of input image respectively.[16]

Step 3. Lexicographically Sorting: In this step lexicographic sorting is performed on the rows of matrix A. Now, in place of comparison of the pixel representation DWT coefficients for each block are being compared, if two consecutive rows of the sorted matrix A are found, the algorithm stores the positions of the identical blocks in a separate list B and increments a shift-vector counter C.

Step 4. Normalized shift vector Calculation: Now shift vector is calculated for a suspected pair of blocks, which are at the same vector distance from the corresponding block[8]. The shift vector v between the two matching blocks is calculated as

$$\mathbf{v = (v1, v2) = (x1 – y1, x2 –y2)}$$

Where (x1, x2) and (y1, y2) are the positions of the two matching blocks.

After that shift vectors v are normalized, because the shift vectors –v and v correspond to the same shift. Then we increment the normalized shift vector counter C by one, for each identical pair of blocks:

$$\mathbf{C(v1, v2) = C(v1 ,v2) + 1}$$

All normalized shift vectors are compared with user-defined threshold T, then the algorithm finds all normalized shift vectors v(1),v(2), …, v(K), whose occurrence exceeds a user-specified threshold T.

$$\mathbf{T: C(v(r)) > T \text{ for all } r = 1, …, K.}$$

Step 5. Match block detection: To identify the segments that might have been copied and moved, the matching blocks that contributed to that specific normalized shift vectors are colored with the same color. Thus the threshold value T is related to the size of the smallest segment that can be recognized by the algorithm.

VI. CONCLUSION

In this paper different methodologies of image forgery detection have been surveyed and discussed about. All the approaches and methodologies talked about in this paper have the capacity to recognize fraud. In any case, a few algorithms are not viable

regarding identifying actual forged region. On the other hand some algorithms have a time complexity problem. So, there is a need to develop an effective (efficient) and accurate image forgery detection algorithm.

REFERENCES

[1] B L.Shivakumar, Lt. Dr. S.Santhosh Baboo "Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods "Global Journal of Computer Science and Technology Vol. 10 Issue 7 Ver. 1.0 September 2010.

[2] Sarah A. Summers, Sarah C. Wahl "Multimedia Securityand Forensics Authentication of Digital Images" http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummersWahl.doc.

[3] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copymove forgery in digital images," Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 2003.

[4] A.C.Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, New Hampshire, USA: TR2004-515, 2004.

[5] G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," IEEE International Conference on Multimedia & Expo, 2007.

[6] "Detection of Region Duplication Forgery in Digital Images Using SURF" B.L.Shivakumar and Lt. Dr. S.Santhosh Baboo IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[7] Sunil Kumar, P. K. Das, Shally. "Copy-Move Forgery Detection in Digital Images: Progress and Challenges" International Journal on Computer Science and Engineering (IJCSE) February 2011.

[8] Amanpreet Kaur Savita Walia Krishan Kumar Comparative Analysis of Different Keypoint 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/IEEENoida, India.

[9] 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/IEEELondon, United Kingdom.

[10] 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.

[11] 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.

[12] 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/IEEEShah Alam, Malaysia.

[13] 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.

[14] Gül Muzaffer Eda Sena Erdöl Güzin Ulutaş A copy-move forgery detection approach based on local intensity order pattern and patch match 2018 26th Signal Processing and Communications Applications Conference (SIU) Year: 2018 ISBN: 978-1-5386-1501-0 DOI: 10.1109/ IEEE Izmir, Turkey.

[15] 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.

[16] A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," Multimedia Tool Appl., Vol. 51, no. 1, pp. 133-62, Jan. 2011.