STM JOURNALS

**Journal of Artificial Intelligence Research & Advances**
ISSN: 2395-6720
Volume 6, Issue 3
www.stmjournals.com

# A Review on Digital Image Forgeries and Their Detection

***Bismah Rafiq[1,*], Sheikh Riyaz-ul-Haq[2]***
[1]Student, Department of Information Technology, Central University of Kashmir, Jammu and Kashmir, India
[2]Assistant Professor, Department of Information Technology, Central University of Kashmir, Jammu and Kashmir, India

***Abstract***

*In today's digital era due to the availability of large and editing tools which are easily available tempering images and changing the content of images have become the easy task. The image is manipulated in such a way that the viewers cannot detect it. Due to this, more work is being done on the internet and almost all information is conveyed by images. So the important task is to check the authentication of the image and check whether the image is original or forged. There are various techniques which we can detect the forged image. This review paper will stick to these forgery techniques. The techniques which will help us to detect the forged images are pixel-based, format-based, geometric-based, camera-based and physical-based techniques.*

***Keywords***: *Camera-based, forged image, forgery, manipulation, physical-based, tempering*

****Author for Correspondence*** E-mail: bismahrafiq1@gmail.com

## INTRODUCTION

"A picture is worth a thousand words", a chines proverb which is became popular in 1990s in all magazines and newspapers. This proverb shows that the power of the image is so high that it can describe the complex form in a simple and efficient manner. Any information which is only conveyed using text cannot be as interesting and informative as to when it is done with the help of an image. In today's digital era storing of information has become an easy task because of the images. Due to advancement in technologies, security has become a more challenging task. With the growth of technologies, the manipulation of images has become an easy task. The software like Adobe Photoshop, Adobe Sky Replaces, Face App, etc. help to manipulate image without any sign of tempering left behind. This software is free, easily available and already installed in our smartphones. The manipulation of the digital picture with the aim of hiding some important or irrelevant information from it is called image forgery. History of image forgery started in the 1980s when the image of Hippolyte was published in newspapers. He himself produced its own fake image of commuting suicide because of frustration that he was not getting recognition. By this, the new process of manipulating pictures was discovered by him. This was also independently discovered by Dagurre and Talbot in 1839 [1].

Manipulation of images is not new, but it gained popularity when we shift in the domain from paperwork to paperless work which payed way for more technological enhancement. Nowadays the data is stored in digital format in government as well as in private sectors which has become an important task for security challenges. The documents, voice data, files, images are all easily manipulated. So security has main concern over here with wide interest over it, researches are detecting doctored images as well as other information from this [1]. The researchers are working day and night in the area of forensics. There are various forgery techniques by which forgery in the images can be detected like a pixel of which image is made of, camera use for imaging, the format in which image is

 

stored, a technique based on physics and geometry of images.

Before we move towards the techniques for detecting the image forgery, we will look towards the types of digital image forgeries. Any sort of changes done in the image like trying to hide some region in the image or trying to add something in the image without leaving a sign of tempering is called as image forgery. There are three categories by which image forgery is done which are discussed below.

**Image Retouching Forgery**

This is one of the most common methods used by the entertainment and media industries. What happened in this forgery is that a certain part of the image is changed like the color of skin, removal of wrinkles, and color of the dress. There is no major change which occurs in this type of forgery as in Figure 1.

**Copy-Move Forgery**

Cloning is another name to copy-move forgery where we copy a certain part of the image and paste that part on the other region or location of the same image as in Figure 2. Copy-paste forgery is used to hide some important information in the image. The texture properties like color do not change since the copied part comes from the same image and this leads to temper detection which is a challenging task [2].

**Image Forgery Using Splicing**

In this type of forgery, a composite image is made of joining two or more images as in Figure 3. In splicing post-processing operation is needed on the spliced region so that surrounding boundaries are not visible. The forged image undergoes some geometric transformation like stretching, skewing, etc. so that tempering is not visible to necked eyes.

## VARIOUS TYPES OF DIGITAL IMAGE FORENSICS TOOLS

When tempering is done in the digital images it leaves its traces. Due to the availability of tools and software, it is not visible to naked eyes but can be detected with the help of various forgery tools. There are two common digital image forensic approaches active technique and passive technique also called a blind technique. In the active method, watermarks and digital signatures are immersed inside the original image by which the authenticity of the image is proved [1]. But its main limitation was that the embedded watermark must be immersed by the device (camera) which is used to take the picture. This is not possible because all devices are not capable of doing so. Also, if we embed watermark ourselves it will degrade the quality of the image.

Another approach is a passive approach or blind approaches. When we do tempering in an image, it leaves traces on it as it goes through various forms of attacks. If these attacks are known, we can detect the forgery. The image forgeries tools have been grouped into five categories.

1. Pixel-based technique
2. Camera-based technique
3. Format-based technique
4. Geometric-based technique
5. Physical-based technique

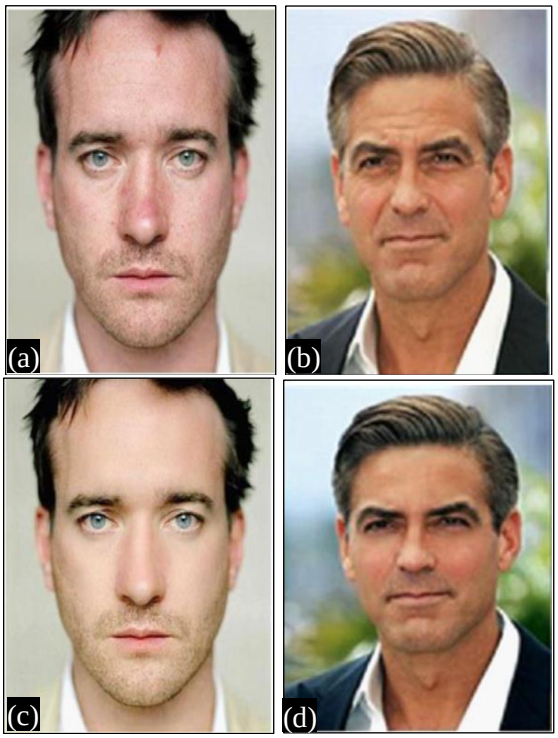


***Fig. 1:*** *Examples of Photo Retouching before the Top and after Bottom [1].*

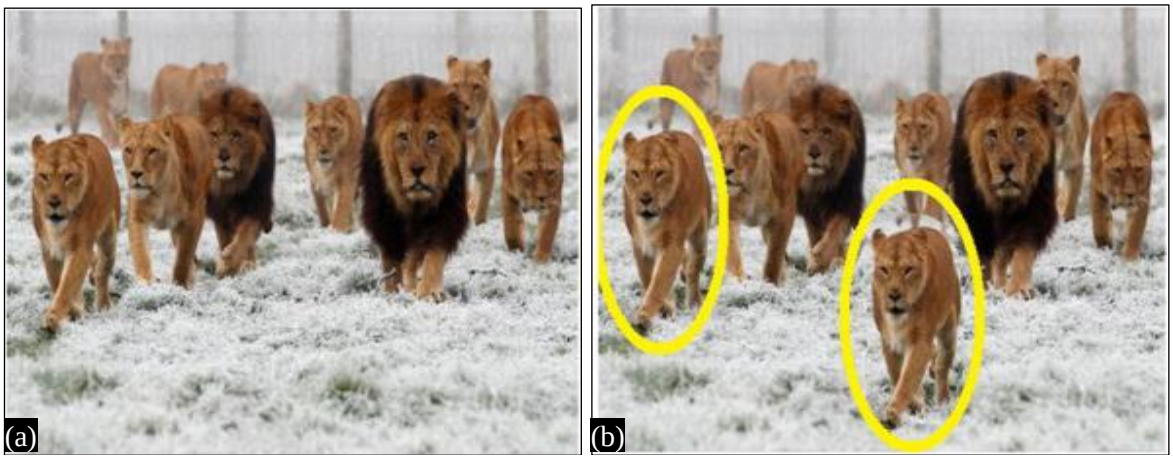


***Fig. 2:*** *Example of Copy-Move Forgery [3].*

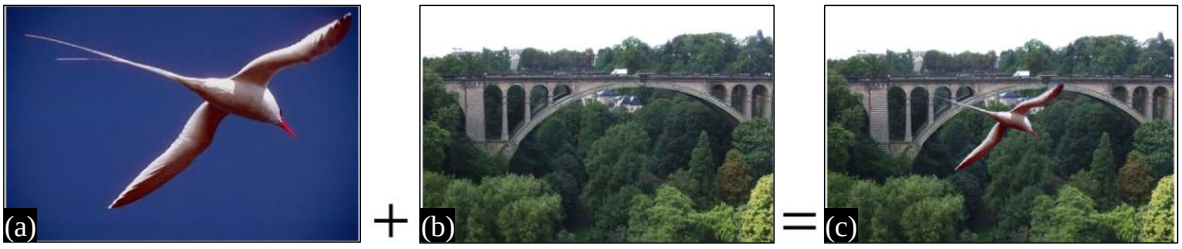


***Fig. 3:*** *Example of Image Forgery Using Splicing [4].*

**Pixel-based Technique**

Pixels are a basic block which built the image. The image is made of pixels and there is a correlation among the pixels so any manipulation is done in the image it will change the pixel correlation. Hence, image forgery can be detected if can detect the changes in the pixel correlation. We can categories pixel-based technique in following three types to detect the various forms of tempering.

***Cloning***

Cloning is one of the most common techniques used for the tempering of images. It is also called as copy-paste in which we copy a certain part of the image and paste that part on the other region or location of the same image. Since the size and location of the copied are different, hence, it is almost impossible to search the entire cloned region. Two algorithms are designed by researchers to detect cloning [2]. First one is the discrete cosine transform (DCT) [2]. DCT is applied to the image and duplicate part is detected. After applying DCT the coefficient are sorted lexicographically and arranged. After that, the similar blocks are grouped which have the same spatial balance image. By this duplicated region is detected. The second algorithm is principal component analysis (PCA) [5, 6]. It is similar to the DCT approach and is done on a small image block of fixed size. The blocks are then arranged in lexicographical order and the duplicate region is detected.

***Resampling***

Resampling is another type of pixel-based technique. When an image is manipulated, it should be done in a way that it is properly rotated, scaled and stretched [7]. By doing this, the relation among the pixels gets distorted or we can say that new correlation among the pixels with a neighbor which are specific and periodic. The new correlation among the pixels will not be normal and so the occurrence of these unordered pixels can detect the manipulation of images. Interpolation is applied to smooth the images. By use of the interpolation algorithm, linear dependencies are induced among the group of neighboring pixels. This dependency wills extent due to the length of the periodic cycle which will depend on the function of resampling rate. The periodic artifacts are used by using linear predictor to detect resampling.

This approach is used by Fraid which calculates the weighted sum of each sample values of its neighbor samples.

***Splicing***

Sampling is a method by which two or more images are joined to form a single composite image. The sum of two sinusoids signals is considered in the bi-spectral analysis. When a signal is passed through non-linearity it induces new harmonic. This new harmonic is correlated with frequency and phase. It is detected that a new harmonic which is introduced as a sum of distinct higher order correlation between the two individual harmonic which will be used to detect the correlation [8]. If we are able to detect such higher order correlation, which is usually weak in natural signals we can say that image is tempered [9].

**Camera-based Technique**

When an image is being clicked by the camera, it goes through many processes before it is being stored. So there are different camera artifacts which occur in the image. Any inconsistency among them can be used to detect the forgery. We can categories camera-based technique in following three types to detect the various forms of tempering.

***Color Filter Array***

The digital camera used now days is composed of three channel consisting of three different color bands that are red, green and blue. The equipment used in these digital cameras is either single CCD or CMOS sensor which is capable of capturing colored images by CFA that is color filter array (CFA). The CFA is located on the top of the sensor element. At each location, the only single color pixel is recorded and the other two are estimated by neighbor samples. CFA interpolation is the name given to the process in which we calculate the missing color samples. CFA interpolations are periodic and have a unique correlation. We can use this as a type of digital signature also.

If we first know the form of specific periodic correlation then we can determine which pixels are correlated with the neighbor pixels. Secondly, the specific form of correlation can determine if it is known which pixel is correlated but both are not possible practically. The author has described how both can be determined and which pixels are not CFA interpolated [10]. The author has employed EM algorithm which can be calculated by two iterative steps.

In the expectation step, which is the first step, the probability of each and every pixel which is being correlated with the neighbor, and the second step is maximization step in which specific form of correlation among the pixel is estimated.

The CFA correlation is done with the simple linear model. It is expected that the periodic pattern of pixels in original images have highly correlated with the neighbor so any deviation in the pattern will detect the forgery.

***Camera Response***

There is a relationship between the camera and the measured amount of light which is linear at different sensor element and with the final pixel value. To boost the final image, we use pointwise non-linearity. We can estimate response function by a single image. Thus, any change in response function will tell us about the tempering of the image. The author has noted the fact that each image has skeptical regions which have different device signatures from the other regions if there is splicing done on the image [11]. We can detect the image splicing by image segmentation by use of any segmented tool like Normalization Cuts or Mean Shift. The testing image is divided into different segments by use of normalization cuts [12] then CRF is estimated in every region. To check whether the image is original or spliced the boundary segment which is between the two neighboring regions is calculated. The data sample from one region and CRF from other region are taken and cross fitting is applied, and these are used for representing a boundary segment. We use SVM classifier for calculating the feature vector. The SVM classifier classifies all the segments that are used collectively for concluding whether the image is spliced or original.

***Sensor Noise***

During imaging by the camera, it goes through various camera components. At each component, information is processed by use of the algorithm and this leaves some intrinsic fingerprints [13]. After tempering an image, we use certain operations which include use of filter for filtering image, resampling the components in images, etc. which leaves a mark on the image which speaks about its manipulation and thus can be detected. A classifier is used to detect the tempering by choosing a threshold value. The reference pattern is compared with the manipulated estimation [14].

**Format-based Technique**

The image must be surely preserved for evidence; this is the first rule of forensic analysis. The worst enemy of forensic analyzing is loosy image compression such as JPEG. The loosy compressions have flexibility regarding the percentage up to what extent compression is to be achieved. By these properties, the camera which has been used for imaging can be identified.

***JPEG Quantization***

Generally, the cameras used nowadays are JPEG encoding which is lossy compression encoding technique. This leads to flexibility regardless of the percentage or up to what compression is to achieve. Thus cameras are designed in a way that they can achieve a balance between the compression and the quality of the picture. By this property, we can determine which camera is being used for imaging. The author has described how to use quality and compression so that we are able to find the camera by which image has been taken [15].

***Double JPEG***

When editing is done in the images it first needs to load in the photo-editor software where it is resaved. Since we know the most common format of image storing is JPEG. So when the image is clicked and saved in JPEG and after editing it is again saved to JPEG. The dual nature lossy compression scheme JPEG format will introduce specific artifacts which are not present in the single compressed image. This can be used as evidence of manipulation [16, 17].

***JPEG Blocks***

The basic nature of the JPEG lossy compression is blocked DCT. So it uses each 8*8 pixel block image for transformation and quantization in the form of vertical and horizontal edges. The block pattern gets change when we try to do changes in the image. The author describes that there is a difference within and beyond the block border of the pixel value by featuring of blocking artifacts [18]. The difference across the block is more whereas the difference within the block is less. After tempering in the image is done blocking artifacts which are of the new type is introduced which will not be as the same alignment with the original image boundary. We can calculate the pixel values from four neighbors, where one neighbor is completely within the JPEG block. Now a histogram is made from the entire 8*8 image block where none of these overlap. After that blocking artifact of 8*8 matrix, size is calculated by the mean difference of this histogram. For a compressed image, the matrix will be particular but for the uncompressed pattern. The tempering will change the specific pattern which is proof of manipulation of image. The difference between blocking artifacts matrix of the original and duplicated image will be detected.

**Geometric-based Technique**

There are two geometric-based techniques by which we can detect the tempering of the images.

***Principal Point***

In an original image, there is a point at the center called as a principal point. When tempering is done on the image, the principal point shifts proportionally. When the difference is estimated this can be used as proof of the doctored image. The author [19] has described how we can find the principal point of the camera by the pair of two circles (two eyes) of the image. The author shows how equivalence is estimated between translations in the digital image to shift the principal point.

  

***Metric Measurements***

The author [20] has discussed various tools for projection geometry. These tools will give the real world measurement from a planer surface and way to rectify the planer surface. Some methods are as follows. The first method is polygon of known shape concept. In the second method, vanishing point concept is used. In the third method, the two coplanar circles are used like wheels of cars. In each and every method, estimation is made for the transformation of world-to-image, by the planer which will remove the distortion and measurements are done.

**Physical-based Technique**

In image splicing, where two or more than two images are joined to form one composite image in which it is difficult to match the lightning effect. Since one image is clicked in one lightning condition and another in another lightning condition. Two techniques are designed to see the difference in lightning across the image so the difference will be evidence of tempering.

***Light Direction***

If we see an image, one part of the image is brighter than the other part. This can lead to the assumption that when the light strikes the surface that is the total amount of light which falls on the surface is always in proportional to the perpendicular surface and also to the direction of the light [21]. By this assumption, we can say that 3D surfaces normal to the direction to the light source [22]. Since it is not possible to determine 3D from a single image, the author [23] has taken only 2D surface normal. By this estimation, two components of light can be made out of the three components in the direction of the light source.

***Lightning Environment***

When an image is clicked, there are many types of light present at different angles and at different positions. Thus the image clicked, is created by using multiple light source with multiple lightning environment. We can estimate the low parameter of the complex light environment [22].

## CONCLUSION

In this survey paper, we have presented the different types of forgeries which are as image retouching, copy-paste and image splicing. To detect these types of forgeries there are various techniques which are grouped into five categories. The pixel-based technique is based on the pattern of pixels of which the image is made. This is further classified into three types that are cloning, resampling and splicing. The second technique is a camera-based technique which will utilize the properties of the camera such as CFA, sensor noise and camera response. The format-based technique is a third technique which is based on JPEG lossy compression which uses JPEG quantization, double JPEG and block JPEG techniques to identify the tempered image. The fourth technique which is used for image forgery detection is a geometric-based technique which can be detected by principal point and metric measurements. The fifth and the last forgery detection technique is based on physical of the image as we know the image is taken in a different lightning condition which will be evidence of manipulated image. Since these techniques are used today but researches are working day and night to make more and more techniques for detection of forgery because of the editing tools present nowadays are very strong.

## REFERENCES

1. Qureshi MA, Deriche M. A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication.* 2015; 39: 46–74p.
2. Fridrich J, Soukal D, Lukas J. *Detection of Copy-move Forgery in Digital Images Proceeding on Digital Forensic Research Workshop*. Cleveland, OH, USA. 2003.
3. Kaur G, Manro R. A Brief Review: Copy-Move Forgery Detection. *Advances in Computational Sciences and Technology*. 2018; 11 (7): 567–96p.
4. Qureshi MA, Deriche M. A bibliography of pixel-based blind image forgery detection techniques. *Signal Processing: Image Communication*. 2015; 39: 46–74p.
5. Katz J, Menezes AJ, Van Oorschot PC, Vanstone SA. *Handbook of applied cryptography*. CRC press; 1996.

6. Popescu AC, Farid H. *Exposing digital forgeries by detecting duplicated image regions*. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004–515; 2004.
7. Popescu AC, Farid H. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on signal processing*. 2005; 53 (2): 758–67p.
8. Farid H. Detecting digital forgeries using bispectral analysis, Artificial Intelligence Lab Publication, Technical Report AIM-1657 MIT AI Memo, 1999.
9. Yang C, Duraiswami R, Gumerov NA, Davis L. Improved fast gauss transform and efficient kernel density estimation. *In null*. 2003; 464p.
10. Popescu AC, Farid H. Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*. 2005; 53 (10): 3948–59p.
11. Hsu YF, Chang SF. Image splicing detection using camera response function consistency and automatic segmentation. In: *IEEE International Conference on Multimedia and Expo*. 2007, Beijing, China July 2. pp. 28–31.
12. Shi J, Malik J. Normalized cuts and image segmentation. *Departmental Papers (CIS)*. 2000; 107p.
13. Gou H, Swaminathan A, Wu M. Noise features for image tampering detection and steganalysis. In: *IEEE International Conference on Image Processing*. San Antonio, TX, USA 2007, Sep 16. Vol. 6, pp. VI-97.
14. Chen M, Fridrich J, Lukáš J, Goljan M. Imaging sensor noise as digital x-ray for revealing forgeries. In: *International Workshop on Information Hiding*. Springer, Berlin, Heidelberg. 2007, Jun 11. pp. 342–358.
15. Lukáš J, Fridrich J. Estimation of primary quantization matrix in double compressed JPEG images. In: *Proc. Digital forensic research workshop*, California, USA. 2003, Aug 5. pp. 5–8.
16. Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: *Proceedings of the 7th workshop on Multimedia and security*. New York, NY, USA. 2005, Aug 1. pp. 1–10.
17. Johnson MK, Farid H. Exposing digital forgeries through chromatic aberration. In: *Proceedings of the 8th workshop on Multimedia and security*, Geneva, Switzerland. 2006, Sep 26. pp. 48–55.
18. Luo W, Qu Z, Huang J, Qiu G. A novel method for detecting cropped and recompressed image block. In: *IEEE International Conference on Acoustics, Speech and Signal Processing*.2007, Apr 15. Vol. 2, pp. II-217.
19. Johnson MK, Farid H. Detecting photographic composites of people. In: *International Workshop on Digital Watermarking*. Springer, Berlin, Heidelberg. 2007, Dec 3. pp. 19–33.
20. Johnson MK, Farid H. *Metric measurements on a plane from a single image*. Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006–579; 2006.
21. Alam S, Ojha D. A Literature study on Image forgery. *International Journal of Advance Research in Computer Science and Management Studies*. 2014; 2 (10): pp. 182–190p.
22. Nillius P, Eklundh JO. Automatic estimation of the projected light source direction. In: *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. Kauai, HI, USA, USA 2001Vol. 1, pp. 1076–1083.
23. Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. In: *Proceedings of the 7th workshop on Multimedia and security*. New York, NY, USA 2005, Aug 1. pp. 1–10.

**Cite this Article**
Bismah Rafiq, Sheikh Riyaz-ul-Haq. A Review on Digital Image Forgeries and Their Detection. *Journal of Artificial Intelligence Research & Advances*. 2019; 9(3): 37–43p.