Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology [ICECA 2019]
IEEE Conference Record # 45616; IEEE Xplore ISBN: 978-1-7281-0167-5

Digital Image Forgery Detection Techniques: A Comprehensive Review

P. B. Shailaja Rani
M. Tech Scholar, Department of CSE
Vardhaman College of Engineering
Shamshabad, Hyderabad, Telangana, India
pbsr94@gmail.com

Ashwani Kumar
Associate Professor, Department of CSE
Vardhaman College of Engineering,
Shamshabad, Hyderabad, Telangana, India
ashwani.kumarcse@gmail.com

***Abstract*— The image forgery techniques are used to provide the particular image in the form of computerized pictures with no errors in capturing of digital image information which shows the original image. While compared to normal images the edited images are difficult to find out the forged images. The image should maintain the authenticity and integrity to secure the picture from unauthorized users. In this paper, we have compared the digital image forgery and JPEG is the most common format used by the photographic images and the digital camera devices. These operations are performed in an adobe photo-shop using with the content of image security to restore some digital image with an authenticity and integrity to detect the digital image forgery using active and passive techniques.**

Keywords*— *Digital Image Forgery, Digital Image, Image Security, Classifications.

I. INTRODUCTION

In this modern age we all are aware about the importance of digital technology. Digital image plays a vital role in many applications. At present, the digital technology has the integrity of the image. Over the past years the digital images of the field have emerged to restore some images. In this digital watermarking is one of the solutions to image authentication problem. Here the digital watermarking means hiding information in some text or image [1]. This is one of the copyright techniques to prove the ownership of the image. Tampering images are used to detect the image forensic tools that are only capable of digital cameras that should not rely on watermarks.

In nature the digital image forgery does not differ any image to compare to any conventional image forgery. Normally the digital images are dealing with the digital forgery [2], by using of photographs. One Can use some software tools by that the digital images carry the powerful computer graphics, Adobe Photoshop in this which we edit software's, and coral paint shop.

Some of the three main causes which are categorized in the process of providing the fake images, that are re-sampling, image splicing, and copy-move detection. One of the important processes of image is image security and it is a way to secure your home and business against crime and avoid becoming another statistic.

This paper is organized as follows: The first section provided the introduction of the digital image forgery detection. The second section shows the classification of image forgery techniques. The third section demonstrates an algorithm for creating a digital image. In the fourth section, rotation angle and rotation images are shown. In the fifth section contain the related work of digital image forgery techniques. Finally, the fifth section concludes the survey paper.

- *Detecting the forgery:*

In the modern era of digital photography taken from the digital camera is used to detect the digital images. One of the software tools is used with an Adobe photo - shop with the dimension of image editor. i.e. the protection of each image used with the help of image filters in the adobe photoshop [2-3].

II. CLASSIFICATION OF IMAGE FORGERY TECHNIQUES:

This section provides some important techniques that are commonly used to detect the image forgeries.

A. Format based image forgery

Format based image has its unique property under the lossy compression [4] that can be exploited for the forensic analysis.

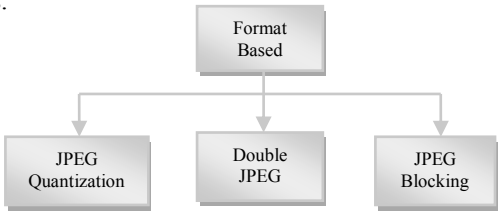

Fig. 1. Format Based Image

- *JPEG quantization:*

The image in which we will provide the JPEG (joint photographic expert group) format that the first image is converted into an RGB image to luminance or chromatic space. These values change according to the low and high compression rates these JPEG present 192 values representing the RGB channels. The quantization achieved by the DCT (discrete cosine transformation) methods [5]. The important factor of the JPEG quantization is JPEG compression that shows the brief:

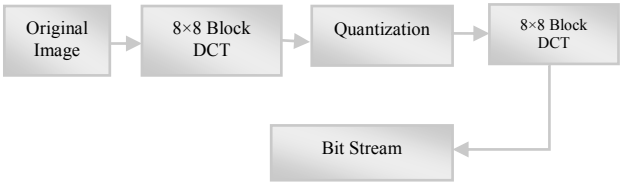

Fig. 2. JPEG Compression

The JPEG compression using 8×8 block the formula is:

$$Di,j=\sum_{k,l=0}^{7} akl(i,j)bkl \quad (1)$$

- *Double JPEG:*

In these both original image and the modified images are stored and it is widely applied it is likely for the image undergoing double JPEG compression to be tampered. It provides important clues for the image forgery detection [5].

- *JPEG blocking:*

In these blocking JPEG has a common factor for digital image compression, these JPEG blocks provide 8 by 8 pixel block which are used with the DCT pixel format that will reduce the file size in the form of Y'CbCr color space [6].

B. Pixel based image forgery

Pixel based image emphasis on pixels when the image is perfectly concern with some filters, it provides some techniques for detecting i.e. cloning, re-sampling, splicing.

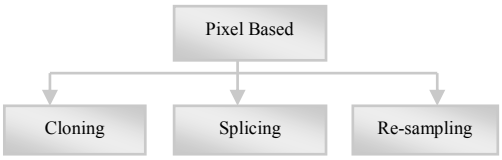

Fig. 3. Pixel Based Forgery

- *Cloning or copy-moved image:*

The main use of the image manipulation is to provide duplication of the picture which the person can identify the object in screen. There are two types of algorithm to detect cloned image regions, i.e. PCA (principal component analysis) and DCT. In copy-move the image is copied and that the image will be pasted to another region. These copy-move image provide two techniques that are active and passive, In Active the hidden information is formed in the digital image that embedded with information that will identify the source of the image. In passive, there are no tamper images [7] and it does not require any information about the picture.

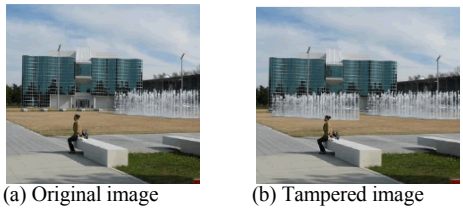

Fig. 4. (a) Original image (b) Tampered image

- *Re-sampling:*

It provides any specific correlation between neighboring pixels; if any, known pixels combined with some neighboring images, and then the particular form of correlating the neighboring are easily performed. We have two steps of iteration algorithms to solve the re-sampling problem. I.e. EM (expectation/maximization) is used.

- *Splicing:*

Splicing performs if two or more images are providing into a single pixel. If splicing is done, then it will disrupt higher order statistics, which results in tampering.

C. Camera based image forgery

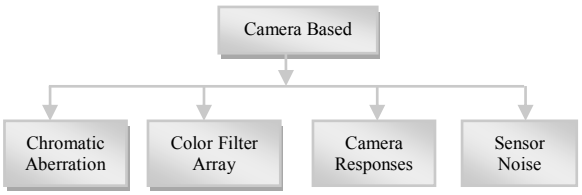

Fig. 5. Camera Based Image Forgery

- *Chromatic aberration:*

It is an existing imaging system, the single point on the sensor to provide the light rays which we can see in lens though the optical systems, they are failing to explain on lights with the wavelengths, thus the resulting effect is called chromatic aberration.

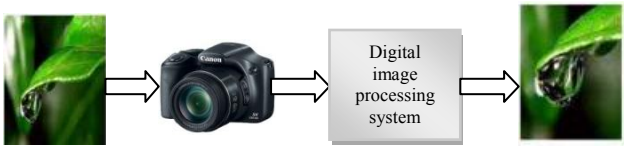

Fig. 6. Digital Image Processing

- *Color filter array:*

Only one-color picture is recorded in each pixel location and another two samples are formed in the neighboring samples, then it estimates 3 channels that are RGB, which the pixels is combined with the other neighboring pixels [7-8].

- *Camera responses:*

The digital cameras are mostly linear it has the relationship with the amount of light measured that provide the corresponding pixel value of the image and from each sensor element we get the resulting image which is tampering [9].

- *Sensor noise:*

Noise on the camera has a strong influence on the maximum responsively and the dynamic range of a camera source has the sensor noise in its light itself, and it has a very high frequency or low power voltage [10]. The computer memory has some digital frames that move from the camera sensors and later it to the quantization process.

D. Physical image based image forgery

Whenever the image is created with some splicing then the individual images are difficult to correlate the lighting effects.

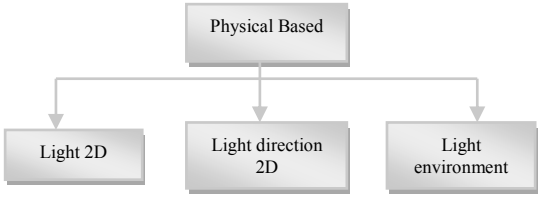

Fig. 7. Physical Image Forgery

This technique is used for providing the lighting environment. The technique based on the 3-dimension of lighting the physical object [9-10]. Lighting is an important factor for capturing an image.

E. Geometric image based image forgery

The basic use of the geometric based is principal point. The projection will measure the image plane that is in the center of the image that place the object over the world [10] and their position relative to the camera.

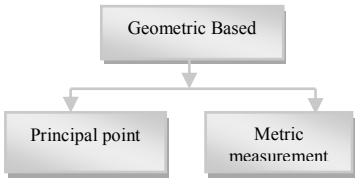

Fig. 8. Geometric Based Forgery

Several forensic techniques have been provided by the lexicographical sorting with row and column vectors that are used to detect the forged region.

➢ *Image Forgery detection techniques*

Forgery detection techniques having two types that are Active technique and passive technique. In an active technique this requires only pre-embedded information. Some of the popular methods are digital watermarking and digital signature, which will used in active technique.

Passive method is also popularly known as blind method, it is non intrusive technique that means no need to pre-embedded technique, the method of an image its user authentication and integrity and also it doesn't perform any visual clues to detect the tampering of images which certain the noise consistency and etc.

III. ALGORITHM FOR CREATING AN IMAGE

The flowchart for creating an algorithm has been shown in the figure below.

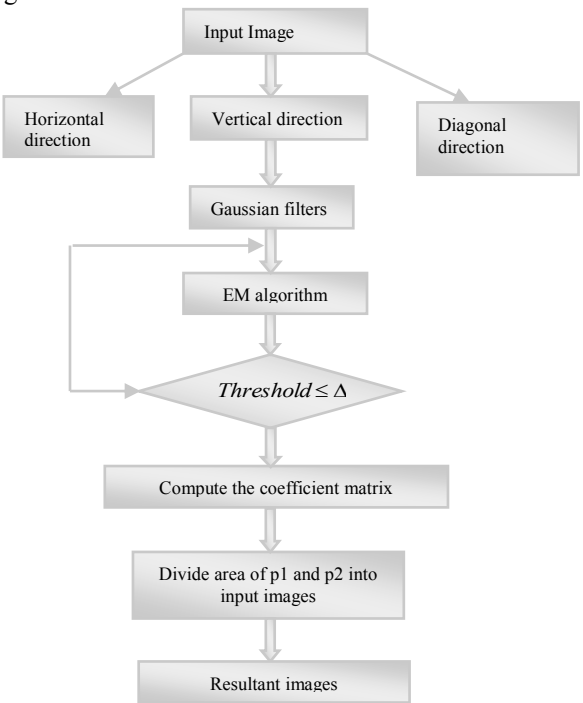

Fig. 9. Flow Chart For Creating An Algorithm

➢ *Steps for creating an algorithm*

1. The digital image that forms in a grayscale image for detecting the interpolated images (512×512) image pixel.
2. We use a Gaussian low pass filter to blur the picture thus it says whether it is dark or brightening of an image.
3. To adapt the region that expectation-maximization (EM) algorithm, the coefficient of the image is estimated in digital forgery and this should be clearly determined.
4. Finally the resultant images are estimated.

IV. ROTATION ANGLE ESTIMATION FOR ROTATED IMAGES

The rotation angle is a factor which works with the frequencies between the rotating images, and provides the interpolation in a spectrum of edge map, by rotation we detect the fake image objects in geometric operations [11] in different process sequence, e.g. zooming, repeating, and rotating.

Rotation angle:

$$i' = i\cos\theta - j\sin\theta$$
$$j' = i\sin\theta + j\cos\theta \quad (2)$$

Here i'= Original image
J'=Intermediate image

The above formula calculates the rotation angle for the digital image, which is to identify the forged image.

By separating some images into blocks, the detecting images of recycling and rotation that perform in each block of the images which are converted to original images, [12] we can relatively identify the forged images.

Fig. 10. (a) Original image (b) Forged image

An altered image is to improve the appearance that cannot be considered through the images it has been altered from the original image [13-14]. Detecting the type of forgeries are becoming the serious issues, we have various forms to detect the forgery to identify the original image [15-16].

V. RELATED WORK

In this section, we have reviewed various research papers related to digital image forgery detection techniques. We also discussed the pros and cons of this technique.

M. Ali Qureshi, M. Derich [17] et al. Proposed copy-move forgery detection technique. The method is to describe the DCT blocks & DWT. It provides the FMT (Fourier Mill-en transformation) overlapping the block of image features be extracted. There obtain the features are robust to rotate, scaling, rotating, noise addition and JPEG compression. Lexicography sorting is added to neighboring block and counters.

Shashank Sharma et al. [18] proposed passive forensic technique for detection on copy-move an attack on digital videos. The method video forgery classified in two ways, that is active and passive it depends on the presence of the original video or which may exist on digital watermarking the video which provide the frame is MPEG format with the process of pixels. The process is in novel technology to detect spatial, temporal forgery which is interrelated to the field of inter and intra frame motion to detect frame insertion and deletion, the method needs a grayscale image so that RGB image that converted to a grayscale image.

Dhanya R, R Kalai Selvi [19] et al. Proposed a method of state of the art review of copy-move forgery detection technique. The method to figure out the pasted or copied image from the original image, this approach is mainly robust for many applications like Gaussian noise detection technique and compression on rotation, scaling, re-sampling etc. in this vector algorithm by applying principal component transformation (PCT). The forgery detection that analyzes the block similarity called k-d tree representation this method suggests the segmenting the original image into non-overlapping irregular block adaptive.

Navpreet Kaur Gill, Ruhi garg [20] et al. Proposed a method is digital image forgery detection techniques. They reduced the issues of image authentication in many areas like medical sciences, administrations, and the forgery detection, which determines the genuineness of picture that should be authentic. The process depends on two types, that is active and passive. The method generalized schema of the image forgery is to be identified in block and key-point based techniques. One of the important technique Brute force method is used, the image process is compressed in JPEG format which determines the undergoes the artifacts of image forgery.

Wing commander Nimit kaura [21] et al. Introduced the analysis if SIFT & SURF features for copy, move image forgery detection. This method is to detect and locate the forgery detection techniques that are categorized in two different forms. The first is key-point and another is block based forgery detection. In which they mainly used (SIFT, SURF, DWT, DCT and SVD) algorithms to detect the forgery which relatively performed the Gaussian function in the image. This method works well, even if the image is extremely compressed.

Wang Zhom [22] et al. Proposed a technology for digital image forgery based on blocking artifacts, as the author describes a situation to detect by digital forgery by correct the inconsistence of the JPEG blocks and measures. DCT method transformation and quantization table are two main parts in JPEG encoding process. To trace of image forgery is used to check image forgery.

Ms. Jaysree charpe and Ms.Antara Bhattacharya [23] et al. Proposed is revealing image forgery through image manipulation detection. The Author presents different techniques used for detecting global contrast enhancement and copy-paste forgery. The technology of global enhancement, which is based on global calculations. This is represented through JPEG compression against robust with the presentation of the preprocessing size of the image forgery.

Parameswaran Nampothiri and Dr. N. Sugitha [24] et al. Proposed DIF-A threaten to digital forensics. In this the passive (blind method) technique is used to detect the forgery technique. By changing some pictures in the Photoshop.

MD. N. Nazi and Ashrat Y. A Maghari [25] et al. Proposed image forgery detection. This will combine the forgery detection algorithm SVM, DCT expanding block-based algorithm. The aim to provide the proper algorithm among the Fourier transformation. The algorithm which shows the high accuracy with DCT and has the lowest accuracy.

Ashwani Kumar et al. [26-29] proposed different buyer-seller watermarking protocol to provide secure and private transaction between the communicating parties.

VI. CONCLUSION

In this paper, the different methods of the digital image forgery detection techniques have been discussed. This technique is used to identify the fake image methods. JPEG is one of the devices that all the images are available in this format that provides with the help of Adobe Photoshop. The image should maintain the authenticity and integrity to secure the picture from unauthorized users to detect the image and we detect the image with active and passive techniques, for example, splicing, re-sampling and copy-move, etc. this is the easiest way to detect the image forgery detection. The performance of different identification methods has been shown by the researchers. A further enhancement of this study is to show the proper tampering of images.

REFERENCES

[1] A.C. Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Traces of Re-sampling”, IEEE Transactions on Signal Processing, 53 (2): 758-767, 2005.

[2] A.C. Popescu and H. Farid, “ Exposing Digital Forgeries in Color Filter Array Interpolated Images”, IEEE Transactions on Signal Processing, 53 (10): 3948-3959, 2005

[3] Chen, W., Shi, Y.Q., Su, W. “Image Splicing Detection uses 2-D Phase Congruency and. Statistical Moments of Characteristic Function,” in society of photo-optical Instrumentation Engineers (SPIE) Conference Series, Feb 2007, Vol.6505.

[4] Shuiming Ye; Qibin Sun; Ee-Chien Chang; “Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact,” IEEE International Conference on Multimedia and Expo, 2007.

[5] M. Stamm and K. Liu, Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints, Information Forensics and Security, IEEE, 2010, Vol. 5, No. 3, Pp.492-506.

[6] Zhang Ting and Wang Rang-ding, Copy-Move Forgery Detection based on SVD in Digital Image, in Proc, 2nd International Conf, Image and Signal Processing (CISP), Tianjin, 2009, Pp. 1-5.

[7] H. Farid, “A survey of image forgery detection,” IEEE Signal Process. Mag., Vol. 26, no. 2, pp. 16–25, Mar. 2009.

[8] R. E. J. Granty, T. S. Aditya, and S. Madhu, “Survey on passive methods of image tampering detection,” in IEEE International Conference on Communication and Computational Intelligence (INCOCCI), 2010, pp. 431–6.

[9] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy-move forgery in digital images,” Proceedings of the Digital Forensic Research Workshop, pp. 5-8, Aug. 2003.

[10] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm,” Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-6, Dec. 2008.

[11] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 1-4.

[12] I. Merino et al., "A SIFT-based forensic method for copy-move, attack detection and transformation recovery," IEEE Trans. Inf. Foren. Sec., Vol.6, no 3, pp. 1099-1111, 2011.

[13] I. Cox, M. Miller, and J. Bloom, Digital Watermarking. New York: Morgan Kaufmann, 2002.

[14] G. Friedman, "The trustworthy camera: Restoring credibility to the photographic image," IEEE Trans. Consumer Electronics., vol. 39, no. 3, pp. 905–910, Jun. 1993.

[15] M. Schneider and S.-F. Chang, "A robust content-based digital signature for image authentication," in Proc. IEEE Int. Conf. Image Processing, vol. 2, 1996, pp. 227–230.

[16] D. Storck, "A new approach to integrity of digital images," in Proc. IFIP Conf. Mobile Communication, 1996, pp. 309–316.

[17] M. Ali Qureshi, M.Deriche, "Copy-Move Image Forgery Detection Techniques" in the Department of Electrical Engineering, King Fahd University of Petroleum and Minerals, Saudi Arabia.

[18] Shashank Sharma, Sunita V Dhavale, "Passive Forensic Techniques for Detection of Copy-Move Attacks on Digital Videos" Computer Science & Engg Department Defense Institute of Advanced Technology Pune, India.

[19] Dhanya R, R Kalai Selvi, "A State of the Art Review on Copy-Move Forgery Detection Techniques" Research Scholar, Noorul Islam University.

[20] Navpreet Kaura Gill, Ruhi Garg "A Review Paper on Digital Image Forgery Detection Techniques" Research Scholar CSE, NITTTR Chandigarh, India.

[21] Wing commander nimit Kaura "Analysis of SIFT and SURF features for Copy-Move Image Forgery Detection" Department of Computer Science Defense Institute of Advance Technology Pune, India

[22] Wang Zhongmei, Long Yonghong, "Digital image forgeries detection based on blocking artifact" National Laboratory of Pattern Recognition Institute of Automatic, Chinese Academy of Science, Beijing.

[23] Ms. Jayshri Charpe,"Revealing Image Forgery through Image Manipulation Detection" Dept. of Computer Science & Engineering G. H. Raisoni Institute of Engg. & Tech. For Women, RTMNU Nagpur, India.

[24] Parameswaran Nampoothiri V, "Digital Image Forgery - A threaten to Digital Forensics" 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[25] Mohammed N. Nazli,"comparison between image forgery detection algorithms", 2017 8th International Conference on Information Technology (ICIT).

[26] Ashwani Kumar, T., Vipin, Mohd, Dilshad, Kumar, Kapil, 2011. A practical buyerseller watermarking protocol based on discrete wavelet transform. Int. J. Comput. Appl. 21 (8).

[27] Kumar, Ashwani, Ghrera, S.P., Tyagi, Vipin, 2014. Implementation of wavelet based modified buyer-seller watermarking protocol (BSWP). WSEAS Trans. Signal Process. 10, 212–220.

[28] Kumar, A., Ghrera, S. P., & Tyagi, V. (2015). Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis. Indian Journal of Science and Technology, 8(35), 1-9.

[29] A. Kumar, S. P. Ghrera and V. Tyagi, "A new and efficient buyer-seller digital Watermarking protocol using identity based technique for copyright protection," 2015 Third International Conference on Image Information Processing (ICIIP), Waknaghat, 2015, pp. 531-535.

TABLE I. COMPARATIVE STUDY OF DIGITAL IMAGE FORGERY DETECTION

S. No	Paper Title	Method Type	Tampering Method Type	Pros/Cons	Year
1	Digital image forgery based on blocking artifacts	DCT	JPEG encoding process	Tracing of the image	2010
2	Image forgery detection	SVM-DCT	Fourier algorithm	The time complexity is high	2014
3	Digital image forgery detection techniques	DyWT	Fourier millen transformation	It will overlap in blocking artifacts	2014
4	Forgery (copy-move) detection, digital image using block method	DWT	Lexicographical Sorting and duplication blocks are identified	Good at manipulation of images	2014
5	Revealing image forgery through image manipulation detection	Similarity matching	JPEG compression	JPEG format is compressed	2015
6	DIF-A threaten to digital image forensics	Copy-move	Copy-move region is detected	Tampering method is detected	2016
7	A passive forensics technique for detection in copy-move attack on digital videos	Gray scale method	Intra and inter frame motion to detect the tempering method	Image insertion and deletion is applied	2016
8	State of the art review on copy-move forgery detection technique.	PCT algorithm is used	k-d tree representation	The Gaussian noise detection technique is used to compress	2017
9	The analysis if SIFT & SURF features for copy-move image forgery detection	Key-point and block-based method	SVD algorithm is tampered	The image is easily compressed	2017
10	Key-point based copy-move forgery detection technique	CMFD frameworks	Easy to use software's	Datasets are emphasized	2017