Survey of Copy-Paste Forgery Detection in Digital Image Forensic

Anushree U. Tembe
Department of Computer Science & Engineering, YCCE
Nagpur, India
anushree.tembe17@gmail.com

Supriya S. Thombre
Department of Computer Science Engineering, YCCE
Nagpur, India
supriyathombre@gmail.com

***Abstract*— Nowadays image manipulation plays an important role due to the powerful photo editing software such as Picasa, Photoshop so that it looks like as original. Such tampering with the original digital image is called as image forgery. The detection of image forgery in an image is important so it can be used as legal evidence in investigations such as court and other fields. Many Images are used as genuine proof of any crime and this remains accurate then it will create a problem. Detecting these forgery types is faces problem at present. To find the forgeries in a digital image is the challenging task. Manipulation of an image is the common place with growing widely access to powerful computing graphics abilities. In this paper trying to implement copy-paste image forgery where copied one part from an image is pasted with another image. The finally result is shows the accuracy and efficiency of this technique for detecting copy-paste forgery with translation, scaling, rotation.**

***Index Term* — Image Forensic; tamper detection; copy-paste forgery**

I. INTRODUCTION

Digital image forensic is the process of manipulate or alter a digital image with a plan to deceive other by an act as exact copies of an original image. The improvement in computer graphics technology inventive many digital images editing software such as Photoshop, Picasa etc. This helps to edit the image content without creating any obvious proof of forgery. Nowdays digital images are authenticated and taking their authenticity admitted becoming increasingly difficult in many legal cases such as in the electronic media, the medical profession, financial institutions and social science [1,2, and 3]. The main target of image forgery is to determine whether a digital image is original or not is the big challenge, therefore, we need image forgery detection in many fields for a protection of the copyright and prevention of forgery [4,6].

Digital image forgery detection technique is categorized into two parts are active evidence and passive /blind evidence shows in following Fig.1

In active evidence, the digital images needed some pre-processing operation such as digital signature image and watermarking. In passive evidence does not require watermark embedded or digital signature generated in advance. It detects the duplicated content in forged images without needed proof an original image. A passive evidence is determined the amount and the location of forgery in the image.

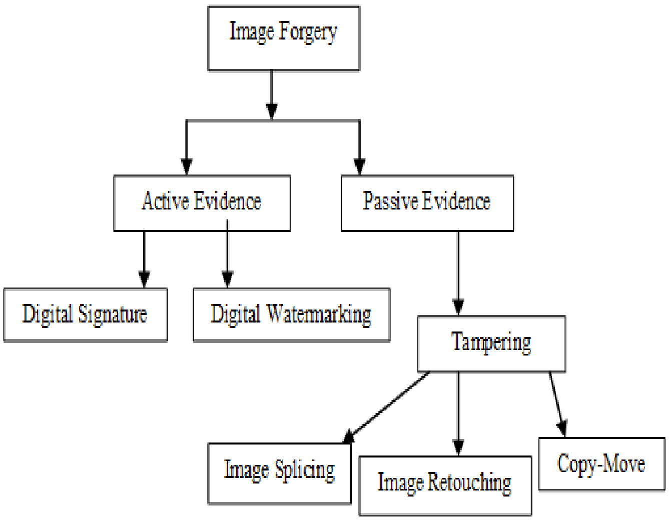

Fig. 1. Classifications of Typical Copy-Move Forgery Detection Techniques

A. *Techniques of Passive Evidence Techniques:*

- Pixel based technique is detect statistical fraudulent activity introduce at the pixel level.
- Format based techniques is preferred statistical correlations introduce lossy compression scheme.
- Camera based techniques are used to handle different artifacts introduce by the different factors such as camera lens, sensor.
- Physically based techniques are detected fraudulent actions in the three different dimensional interactions between the camera, light, and physical objects.
- The geometrically based technique measures the objects in their world positions towards the camera.

There are several cases widely used to manipulate digital images.

A. **Image Retouching**: - This is the process does not significantly change an image but instead enhances or reduces the certain feature of an image. Following Fig. 2 shows the image retouching where the left image is original image and right image forged image or retouched image**.**

Fig. **2**. Image Retouching

B. **Image Splicing**: - Image splicing is the technique that involves a composite of two or more image which is combined to create a fake image. Following Fig. 3 shows the image retouching where the top side image is original two images and bottom side image is forged image or spliced image.

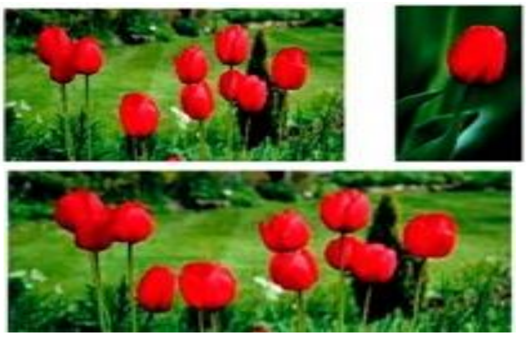

Fig. 3. Image Splicing

C. **Copy-Move: -** In this technique portion of an original base image as its source. Another word, the source, and destination of the modified image originate from the same image. Following Fig. 4 shows the copy-move where the left image is original image and right image forged image or copy-move image.

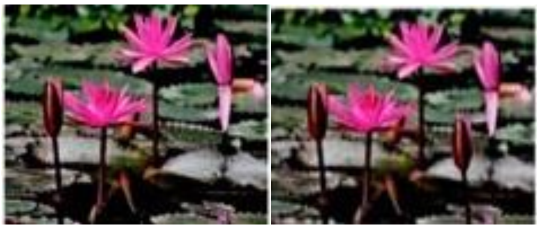

Fig. 4. Copy-Move

D. Morphing: - This technique is used to transfer the one-person image from another person image by using a continuous transition between two images. Image Morphing is shown in Fig.5 where the left side is the original image, in middle is forged image and the right side is the original image.

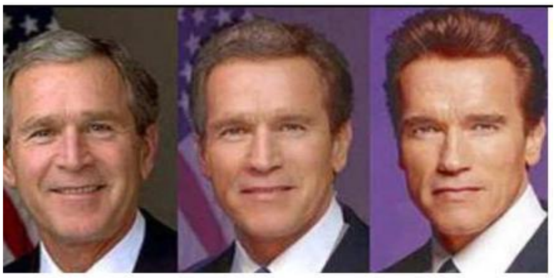

Fig. 5. Image Morphing

The rest of the paper is organized as follows. In Section 2, the typical flow of copy-move forgery detection is described. The overview of copy-move technique detection is provided in Section 3, and in section 4 related work and a comparison table are provided.The conclusion and future scope are drawn in section 5 and section 6.

II. Typical Flow Of Common Copy-Move Forgery Detection

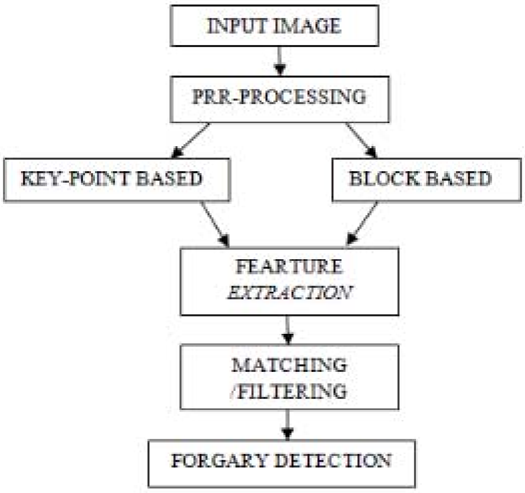

Fig. 6. General Framework of Copy-Move Forgery detection

- Pre-Processing is applied for image conversion from colored image to gray scale, image enhancements to remove the additive noise from input images.
- Feature Extraction is used for a process to extract or finding features from input image for representing the

image better manner. It reduced redundancy in the original image and dimensionality of data.

- Matching or Filtering is the process used to find a higher similarity or matching between feature descriptors and if the similarity between them is found then it is interpreted as there is a duplicated region.
- Forgery Detection or post-processing is the process is used to find as non-authentic image and helps to find out which transformation has been used between copy-moved and its original version.

III. Overview Of Copy-Move Technique Detection

Copy- Move Forgery Detection technique is classified mainly into two approaches:

- Block Based Methods.
- Key-Point based Methods.

Block Based Method.

In the blocked-based method where image separated into small overlapping and nonoverlapping blocks. Then the separated blocks compare with each other for analyzing the matching area and these areas cover through a matching block. However, the main concern with these techniques is required to much time for computation. Also, the most block -based techniques fail when the copied portion of an image goes under some operation such as scaling, rotation, etc.
There are 13 block-based methods and it can be divided four categories: Moment-based (Blur, Hu, Zernike), Dimensionality reduction-based (PCA, SVD, KPCA), Intensity-based (Luo, Lin, Bravo), Frequency -based (DCT, DWT, and FMT).

Key-Point Based Method

In the Key-point based techniques based on identifying and select high-level entropy image region. In this method, the two images compared and applied to find if there is any similarity between them and there is no subdivision into blocks. This technique the key point extracted per feature vectors. The feature vectors are calculated, results are reduced the computational complexity of feature matching. Key-point based approach mainly uses the scale and rotation-invariant feature and descriptor algorithms. Key-point based method includes two algorithms such are (SIFT) Scale Invariant Feature Transform and (SURF) Speeded-up Robust Features.

IV. Related Work

In the last decade, many passive evidence techniques for copy-move forgery have been proposed. Fridrich [1] first introduced a method (DCT) Discrete Cosine Transform of overlapping blocks. The feature vectors are made using coefficients of DCT. The similarity of two blocks is detected after sorting the feature vectors lexicographically. Popescu [2] presented a copy-move forgery detection using an algorithm based on (PCA) Principal Component Analysis which is applied to determined small fixed size image blocks to get a reduced dimensionality.

Li [4] presented an algorithm Discrete Wavelet Transform (DWT) and firstly reduces the dimension of the image by considering only the low-frequency sub-band of Discrete Wavelet Transform result and then size is reduced of the feature vector using Singular Value Decomposition (SVD). A different approach was presented by Wang [6] proposed method is Singular Value Decomposition (SVD) and robust to post-processing techniques and less time complexity. In this method, the correlation is used for copied and pasted areas and for searching similar regions.

Bayram [7] presented Fourier-Mellin transform (FMT) method for forgery detection.FMT is applied to each block and values are finally calculated to form feature vector using single dimensional. FMT features are invariant to translation and scaling in addition to their robust to noise, burring and compression. Ryu [8] introduced Zernike moment method used to localize the tampered region in digital images based on features Zernike moments of circular blocks. These methods are robust to compression, noise, and are most important for blurring and rotation invariant. It is need to detect the copy-move blocks for flat surface of regions. This method is failed to detect scaled copy-move blocks. The major cons moments based technique is their high computational cost.

Another work Bo [11] in 2010 presented a method and used Speeded-up Robust Features (SURF) algorithm. In this method, Hessian matrix is used for the key point detection and description and for assigning the orientation. In 2011, Amerin [12] introduced a copy–move forgery method based on scale invariant features transform (SIFT) algorithm extracts robust features that help to detect if a part of an image was copy-moved and whether it goes through a geometrical transformation.

Another work Zhong [18] introduced a method for forgery detection the low-frequency part of the image performed Gaussian pyramids decomposition. Low-frequency part is the divided by size of the image. The value is computed for the overlapping sub-blocks and then a total count is calculated. In another method, Thajeel [19] discussed the Gaussian pyramid are used for circle block of image dimensions and four features analyzed. The image divided into many fixed sized blocks that and further combined and then calculated the region values through Hu moments.

Kaur [23] introduced a method for image forgery detection method based on LBP and SPT . The experimental result shows that LAB chrominance channels are better suited for image forgery detection than the luminance channel (gray scale) for processing then SPT is used for detecting the rotational part up to 360-degree rotation of forged and LBP channel is for highlights the texture more accurately. Ardizzone [24] introduced a method of forgery detection based on the novel hybrid approach, which compares triangles instead of block or keypoints .In which point interest is extracted from the images and objects are set as connected points of triangles. Triangles are matched according to inner angles shapes, according to color information content, and the vertices of the triangle extracted from local feature vectors and this method is robust geometric transformations.

Later presents the Gabor magnitude of an image was used for feature extraction by Hsu [25] Gabor filter is applied to the blocks of image and blocks of features are extracted by a histogram of Gabor magnitude. Further similarities matches are detected by post processing and sorting. Nirmalkar [26] introduced a method of forgery detection based on the irreconcilable in illumination. Illuminant estimates based on physics and statistics. This method evaluates the authenticity of the human visual system and image depending on indentify and evaluates the forgery parts of the image.

Ferreira [28] presented a method multi-scale behavior knowledge space (BKS) algorithm. The two methods are combined blocked based and key-point based and overcome a disadvantage of this two method an author proposed method which encodes the output combinations of different techniques as a priori probability considering different scales of the training data. Afterward, the missing entries of conditional probabilities are properly estimated through generative models applied on the existing training data.

IV. CONCLUSION

With advancement in the image processing technology, forgery detection method is more demanding in our society. The identification of digital image forgery is important to research topic in crime investigation, harassment, and forensic science etc. Image Forgery Detection technique is used to find out the authenticity of an image. So it is mandatory to find out the image is fake or original. Here with our brief overview of copy-move forgery detection demonstrate that this work is still going on stages and there are lots of potential for future research.

V. FUTURE SCOPE

In future work, more tests will be performed on pictures with a greater quantity of testing samples, with a different scale invariant factor such as additive noise; scaling, stretching, blurring etc. forged part can be included. A comparison of different performance evaluation factors in image forgery detection can also be investigated in future work.

REFERENCES

[1] J. Fridrich, D. Soukal and J. Lukas, “Detection of Copy-Move Forgery in Digital Images, *Digital Forensic Research Workshop, Cleveland*, pp. 19–23, 2003

[2] A. C. Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Duplicated Image Regions”, Tech. Rep. TR2004-515, Dartmouth College, 2004

[3] A. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," *in IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948-3959, Oct. 2005

[4] G. Li, Q. Wu, D. Tu, and S. Sun, “A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD,” *in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China*, pp. 1750-1753, July 2-5, 2007

[5] Z. Ting and W. Rang-Ding, "Copy move Forgery Detection Based on Svd in Digital Image," *in Proceedings of Image And Signal Processing, Cisp'09. 2nd International Congress On*, pp. 1-5, 2009

[6] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast And Robust Forensics for Image Region duplication Forgery," *in Proceedings of Acta Automatica Sinica*, Vol. 35, pp. 1488-1495, 2009

[7] S. Bayram, H. Taha Sencar and N. Memon, "An Efficient and Robust Method for Detecting Copy-Move Forgery," *in IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, pp. 1053-1056, 2009

[8] S. Ryu, M. Lee and H. Lee, “Detection of Copy-Rotate-Move Forgery Using Zernike Moments,” *in Proceedings of Information Hiding Springer Berlin Heidelberg*, pp. 1053-1056, 2009

[9] S. Khan and A. Kulkarni, "Robust Method For Detection Of Copy-Move Forgery In Digital Images," *in Proceedings of Signal and Image Processing (ICSIP), 2010 International Conference on*, Chennai, pp. 69-73, 2010

[10] L. Fitzpatrick and M. Dent, “Region Duplication Detection Using Image Feature Matching,” *in IEEE Transactions On Information Forensics And Security*, vol. 5, no. 4, 2010

[11] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image Copy-Move Forgery Detection Based on Surf," *in Proceedings of Multimedia Information Networking and Security, International Conference On*, pp.889-892, 2010

[12] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "An SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery," *in Proceedings of IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, Sept. 2011

[13] M. Sridevi, C. Mala, And S. Sandeep,"Copy–Move Image Forgery Detection In A Parallel Environment," *in Proceedings of Image And Signal Processing, Cisp'09. 2nd International Congress On*, 2012

[14] V *Christlein*, *C Riess*, *J Jordan*, *C Riess*, *E Angelopoulou*, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *in IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841-1854, Dec. 2012

[15] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *in Proceedings of Information Forensics And Security, IEEE Transactions On*, Vol. 7, Pp. 1018-1028, 2012

[16] Z. Mohamadian & A. Pouyan, “Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions,” *in Proceedings of Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on*, pp. 455-460, 2013

[17] *H. Shah, P. Shinde and J. Kukreja*, "*Retouching Detection and Steganalysis*", *IJEIR, Vol. 2, pp. 487-490, 2013*

[18] L. Zhong and W. Xu, “A Robust Image Copy-Move Forgery Detection Based On Mixed Moments”, *in Proceedings of IEEE International Conference on Software Engineering and Service Sciences (ICSESS*), May 2013.

[19] S. Thajeel and G. Sulong,"A Survey Of copy-Move Forgery Detection Techniques", *Journal of Theoretical and Applied Information Technology*, Vol.70, 10th December 2014.

[20] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *in IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, March 2015.

[21] C. Hsu, J. Lee, and W. Chen, “An efficient detection algorithm for copy-move forgery,” *in Proceedings of Asia Joint Conference on Information Security* (AsiaJCIS), pp. 33–36, May 2015

[22] N. Joglekar, and P. Chatur, “A Compressive Survey on Active and Passive Methods for Image Forgery Detection,” in *IEEE Transactions on Image Processing*, vol. 4, issue 1,2015

[23] H. Kaur and K. Kaur, “Image Forgery Detection using Steerable Pyramid Transform and Lab Color Space”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, August 2015

[24] E. Ardizzone, A. Bruno, and G. Mazzola,”Copy–move Forgery Detection By Matching Triangles Of Key-points,” IEEE Transactions On Information Forensics And Security, Vol. 10, No. 10, Oct. 2015

[25] Chen-Ming Hsu, Chungli, Taiwan, Jen-Chun Lee and Wei-Kuei Chen, “An Efficient Detection Algorithm for Copy-Move Forgery” *in Proceedings of* 10th Asia Joint Conference on Information Security, pp 33-36, May 2015

[26] N. Nirmalkar and S. Kamble, “Illumination Color Classification Based Image Forgery Detection: A Review” *International Journal of Computer Science and Applications*, *8*(1), 2015.

[27] K. Asghar, Z. Habib & M. Hussain , "Copy-move and Splicing Image Forgery Detection and Localization Techniques: A Review," *in Proc.* Australian Journal of Forensic Sciences, Vol. 0(0), pp. 1-27, 2016

[28] A. Ferreira, S.C. Felipussi, C. Alfaro, P. Fonseca, And A. Rocha,” Behavior Knowledge Space-based Fusion For Copy-move Forgery Detection,” IEEE Transactions On Image Processing Vol. 25, No. 10, Oct. 2016