A Systematic Study: Passive Methods of Image Counterfeit Detection Technique

Shashikala S[1]
Department of Computer Science
Assistant Professor,
New Horizon College
Bangalore, Karnataka, India

Dr Lokesh N S[2]
Department of Computer Science
Professor,
Presidency College
Bangalore, Karnataka, India

***Abstract* - With the development of the digital image processing software and editing tools, a digital image can be easily manipulated. Image forgery detection is very important because d. It is a vital process where the images are considered as major proof to alter judgment in various scenarios like court laws. The pixel-based image forgery detection is a blind approach which aims to verify the authenticity of digital images without any prior knowledge of the original image. There are many ways for tampering an image such as cloning, resampling an image, addition, and removal of any object from the image. In this paper we have discussed various passive approach for image counterfeit detection, mainly cloning and splicing techniques.**

Keywords - Image counterfeit detection; cloning;Splicing; Tampering

I. INTRODUCTION

Now a day's, digital images can be easily tampered with widely available editing tools such as photoshop, etc., Image editing has reached a stage that tampering can be done without any trace identification. The increased usage of digital image editing tools made it easier to make the contents of a digital image can be easily edited and modified [1]. It is very difficult to recognize the image is original or manipulated [2]. Therefore, developing techniques to verify the integrity and authenticity of the digital images is very important, especially images are now being presented as supported evidences and historical records in various fields, such as in forensic investigation, law enforcement, journalistic photography and medical images.. Image forgery detection is one of the primary goals of image forensics [3]. The identification of a counterfeit region

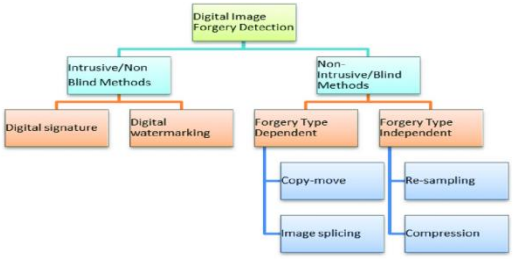


Fig.1: Image Forgery Detection Methods

Blind image forgery detection techniques can be split into five types [4] as shown in Figure 2.

Pixel-based techniques detect algebraic inconsistencies created at the pixel level

The main objective of this paper is:

1. To introduce different approaches of image forgery detection.

2. To analysis on pixel-based image forgery detection.

Digital image counterfeit detection techniques are classified into blind and Non-Blind methods. In the Nonblind approach, the digital image requires preprocessing of image such as watermark embedding or signature generation, which limits their application practice [3].

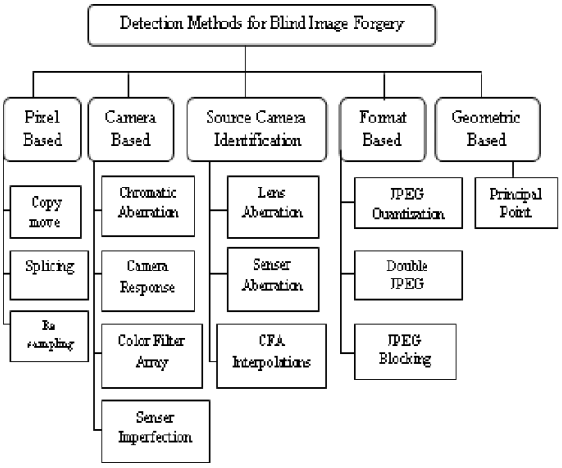


Fig2: Pixel based Image Forgery Detection categories

1. *Pixel-centered image counterfeit detection:*This methodhighlights on the pixels of the digital image. These methods are roughly categorized into four types. We are aiming only two types of methods cloning and

splicing in this paper. It is one of the most common counterfeit recognitionmethods. *Format-centered image counterfeit detection:* Format based methods are a modern type of image forgery recognitionmethod. These methods work mainly withthe JPEG format. These techniques can be divided into three types. If the image is compressed, then it's extremely difficult to detect falsification but these techniques can detect falsification within the compressed image.

2. *Camera-centered image counterfeit detection:* Whenever we capture an image from a camera, the image transfers from the sensor to the memory and it experiences a series of processing steps, like quantization, color connection, gamma improvement, white balancing, filtering, and JPEG compression. These techniques can be divided into four categories.
3. *Source Camera Identification counterfeit detection*:.This techniques supports the lighting environment under which an object or image is captured. Lighting is extremely important for capturing a picture. These techniques are divided into three categories.
4. Geometry-centered image counterfeit detection: Geometry-based detection method make volume of objects within the globe and their position relative to the camera [4].

II. PIXEL-BASEDIMAGE COUNTERFEIT DETECTION

Pixel-based image counterfeit detection is generally categorized into 3 types Pixel-based techniques detect arithmetical abnormalities introduced at the pixel level [1,4].

2.1 Cloning (Copy-Move)

This is the foremost common form of image forgery and this can be also referred to as copy-move forgery. within the copy move a component of the image is copied and pasted somewhere else within the image. The Fig. 3 shows a straightforward example of a duplicate move forgery, where the Prime Minister of Canada, William Lyon Mackenzie, removed King of Great Britain from the initial photograph with the PM and Queen Elizabeth. The image was used on an election poster for the Prime Minister. The goal of this counterfeit was a political propaganda [5].

Fig 3: Example of Copy Move image Forgery

2.2 Resampling

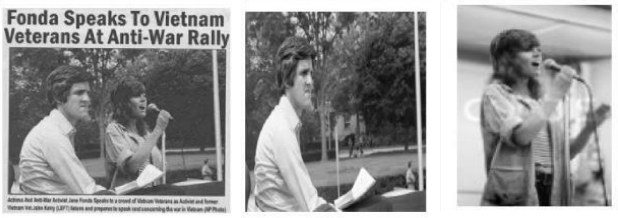
Resampling inevitably introduces some visual artifacts within the resampled image. the most forms of artifacts are sharp edges, and include aliasing, blurring, and edge halos. So, this process has to resample original image into a replacement sampling lattice [6].

(a) (b)

Fig 4: Example of Image Retouching (a) before (b)after

2.3 Splicing

This is one more type of image counterfeit blind approach. In this approach splicing of two or more images is concatenated into a single image [6]. If we have two images (Figure 4), both images are merged into a single composite image (Figure 5) . Which done wisely, the boundary between the spliced regions can be visually hardly noticeable.



(a) (b) (c)

Fig.5 : Example of Spliced Image (a) of Two Authentic Images (b) and (c)

III. EXISTING PIXEL-BASED IMAGE COUNTERFEIT DETECTION TECHNIQUES

There are many approaches that are proposed by various authors for detecting pixel-based image forgery. Figure 6 shows the final process of detecting copy-move image forgery [2, 6-23].

PCA: principal component analysis.

DCT: discrete cosine transforms.

DWT: discrete wavelet transforms

SVD: singular value decomposition.

SIFT: scale invariant feature transform.

SURF: accelerated robust features.

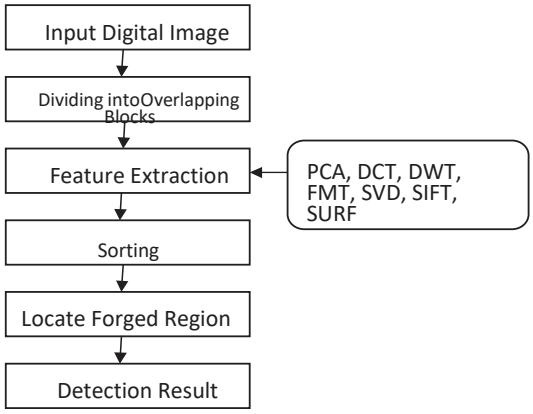


Fig. 6: Block diagram of copy-move image counterfeit detection system

Fridrich et al. [15] proposed a technique for detecting copy-move image forgery. during this method, the image is split into overlapping block for feature abstraction. Authors have used DCT coefficients for feature extraction. Then, the DCT coefficients of blocks are sorted. After graphical sorting, similar blocks are detected, and forged regions are found. during this paper authors perform robust retouching operations within the image. But authors haven't performed the other robustness test.

Popescu et al. [14] proposed a technique for detecting edited imageregions.In this technique PCA is applied on small fixed-size image blocks. They calculate the eigenvalues and eigenvectors of each block. After applying sorting on the computed eigen value and eigen vector, the manipulated regions are automatically detected. This technique is an efficient for detecting a tampered region automatically. The advantage of this algorithm is that the flexibility to detect duplicate region whether the image is compressed or noisy.

Kang and Wei [8] proposed the use of SVD to find the tampered regions in an digital image. during this paper Authors used SVD for extracting feature vector and dimension reduction. sorting is applied on vectors and similar blocks are found to detect forged regions. This algorithm is powerful and efficient.

Lin et al. [16] proposed a fast copy-move forgery detection technique. in this algorithm PCA is used for locating feature vectors and dimension reduction then Radix sort is applied on feature vectors to detect forgery. This algorithm is efficient and works well in compressed images.

Huang et al. [10] proposed the detection of copy-move forgery in digital images using SIFT algorithm. during this paper, authors introduced SIFT algorithm using feature matching. The algorithm detects manipulated region even when image is noisy or compressed.

Li et al. [11] proposed a sorted neighborhood pixelfor detecting duplicate region supported DWT and SVD. during this paper, authors used DWT and decomposed into four sub-bands. SVD was employed in low-frequency sub bands to cut back dimension representation. Then, they applied lexicographical sorting on singular value vector and thus the cast region is detected. They tested greyscale and color images for detecting duplicate region. This algorithm is powerful.

Luo et al. [18] proposed a powerful detection of region duplication in digital images. in this proposed method, image is divided into overlapping blocks then apply the relationship matching on these blocks. The relationship matching identifies the duplicate regions within the image. This method also works within the JPEG compression, Gaussian blurring, and additive noise.

Zhang et al. [19] proposed a innovative approach for detecting copy-move forgery detection in digital images. Authors used DWT and divided the image into four low frequency sub bands and phase correlation is implemented to compute the spatial counteract between the copy-move regions. Then, they applied pixel matching for detecting the solid region. This algorithm works well within the highly compressed image. this may be a very effective algorithm with lower computational time compared with other algorithms.

Kang et al. [20] proposed copy-move forgery detection in digital image. In this algorithm an image divided into subblocks and used improved SVD. Then, relationship matching is performed on the lexicographically sorted SV vectors and the forged region in the images is detected.

Lin et al. [8] proposed an integrated technique for splicing and copy-move image forgery detection. In this algorithm an image is converted into the YCbCr color space. For merging detection, the image is divided into subblocks and DCT is used for feature extraction. For copy-move detection, SURF is used. The algorithm works well on blind image forgery detection techniques.

Qu et al. [7] proposed a way to detect digital image splicing with visual cues. The authors used a detection window and divided it into nine subblocks. VAM (visual attention model) is utilized to identify a fixation point then feature extraction for extracting the spliced region within the image.

Lin et al. [21] proposed a fast, automatic, and fine-grained tampered JPEG image detection technique using DCT coefficient analysis. This algorithm have used DCT coefficient and Bayesian approach for detecting a forged block. Feature mining is applied to remove the forged region.

Cao et al. [25]. proposed a vigorous detection algorithm for copy-move forgery in digital image. this technique used DCT for finding DC coefficient, each block represents by group block and extract feature from each circle block. Searching relationship block sets and find counterfeit region.

N Hema Rajini[26] ,proposed a new image forgery identification method which split with merging and copy move counterfeits simultaneously. At the initial stage, the transformation of the input image to YCbCr channels takes place. Then BDCT and image de-correlation takes place as the pre-processing step. Once the purified features are integrated, the model will be trained using good and forged images. Then, CNN is employed for classifying an image as spliced type or copy-move type. Its powerful method for both copy move and splicing forgery detection methods.

IV. CONCLUSION

In this paper passive approaches of pixel image counterfeit detection have been reviewed and discussed. All the methods discussed in this paper can detect counterfeit region in a digital image. But some methods are not effective in terms of identifying actual counterfeit region. Some algorithms are not effective in terms of time convolution. So, there is a need to develop an effective and accurate image forgery detection algorithm.

V. REFERENCES

[1] J. A. Redi, W. Taktak, and J.-L. Dugelay, “Digital image forensics: A booklet for beginners,” Multimedia Tool Appl., Vol. 51, no. 1, pp. 13362, Jan. 2011.

[2] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, “Fast and robust forensics for image region-duplication forgery,” Acta AutomaticaSinica, Vol. 35, no. 12, pp. 148895, Dec. 2009.

[3] V. Tyagi, “Detection of forgery in images stored in digital form,” Project report submitted to DRDO, New Delhi, 2010.

[4] H. Farid, “A survey of image forgery detection,” IEEE Signal Process. Mag., Vol. 26, no. 2, pp. 1625, Mar. 2009

[5] B. George. (2016, on 29th January, 2017). 12 Historic Photographs that were actually Doctored (14 HQ Photos).Available: http://thechive.com/2012/02/07/12historicphotographs-that-were-actuallydoctored-14-hq-photos/

[6] 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. 4316.

[7] Z. Qu, and G. Qiu, “Detect digital image splicing with visual cues” Lect. Notes Comput. Sci., Vol. 5806, pp. 24726, Jan. 2009.

[8] S. D. Lin et al., “An integrated technique for splicing and copymove forgery image detection,” in IEEE 4th International Congress on Image and Signal Processing (CISP), Vol. 2, 2011, pp. 108690.

[9] X. Kang, and S. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics,” in International Conference on Computer Science and Software Engineering, 2008, Vol. 3, pp. 92630.

[10] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm,” in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, Dec. 2008, pp. 2726.

[11] G. H. Li, Q. Wu, D. Tu, and S. J. 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, Jul. 2007, pp. 17503.

[12] G. H. Li, Q. Wu, D. Tu, and S. J. 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, Jul. 2007, pp. 17503.

[13] M. Ghorbani, M. Firouzmand, and A. Faraahi, “DWT-DCT (QCD) based copymove image forgery detection,” in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 14.

[14] I. Amerini et al., “A SIFT-based forensic method for copymove attack detection and transformation recovery,” IEEE Trans. Inf. Foren. Sec., Vol. 6, no 3, pp. 1099111, 2011.

[15] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy move forgery in digital images,” in Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 58.

[16] A. C. Popescu, and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[17] H.-J. Lin, C.-W. Wang, and Y.-T. Kao, “Fast copy-move forgery detection,” in WSEAS Transaction on Signal Processing, 2009, pp. 18897.

[18] W. Q. Luo, J. W. Huang, and G. P. Qiu, “Robust detection of region-duplication forgery in digital image,” in Proceedings of 18th International Conference on Pattern Recognition (ICPR 2006), Vol. 4, pp. 7469, 2006.

[19] Y.B. Ravi Kumar, C.K. Narayanappa, Dayananda P,”Weighted full binary treesliced binary pattern: An RGB-D image descriptor”,Heliyon, Volume 6, Issue 5,2020,e03751

[20] J. Zhang, Z. Feng, and Y. Su, “A new approach for detecting copy-move forgery in digital images,” in IEEE International Conference on Communication Systems, China, 2008, pp. 3626.

[21] L. Kang, and X.-P. Cheng, “Copy-move forgery detection in digital image,” in 3rd International Congress on Image and Signal Processing (CISP 2010), IEEE Computer Society, 2010, pp. 241921.

[22] Z. Lin et al., “Fast, automatic and finegrained tampered JPEG image detection via DCT coefficient analysis”, Pattern Recogn., Vol. 42, pp. 2492250, 2009.

[23] X. Pan, and S. Lyu, “Region duplication detection using image feature matching,” IEEE Trans. Inf. Foren. Sec., Vol. 5, no. 4, pp. 85767, Dec. 2010.

[24] R. C. Gonzalez, and R. E. Woods, “Digital Image Processing Using Matlab,” Pearson Education India, 2004 .

[25] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copymove forgery in images”. Forensic Sci. Int. Vol. 206, pp. 17884, 2011

[26] Yanjun Cao, T. Gao, and Qunting Yang, ”A robust detection algorithm for copy-move forgery in digital images” Forensic Int. Vol. 214, pp. 3343, 2012.

[27] N Hema Rajini,” Image Forgery Identification using Convolution Neural Network “International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019