IETE Journal of Education

ISSN: (Print) 0974-7338 (Online) Journal homepage: https://www.tandfonline.com/loi/tije20

Pixel-Based Image Forgery Detection: A Review

Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi

To cite this article: Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi (2014) Pixel-Based Image Forgery Detection: A Review, IETE Journal of Education, 55:1, 40-46, DOI: 10.1080/09747338.2014.921415

To link to this article: https://doi.org/10.1080/09747338.2014.921415

Published online: 07 Aug 2014.

Pixel-Based Image Forgery Detection: A Review

Mohd Dilshad Ansari[1], S. P. Ghrera[1] and Vipin Tyagi[2]

[1]Jaypee University of Information Technology, Waknaghat, HP, India,
[2]Jaypee University of Engineering and Technology, Raghogarh, MP, India

ABSTRACT

With the advancement of the digital image processing software and editing tools, a digital image can be easily manipulated. The detection of image manipulation is very important because an image can be used as legal evidence, in forensics investigations, and in many other fields. The pixel-based image forgery detection 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 splicing or copy-move, resampling an image (resize, rotate, stretch), addition and removal of any object from the image. In this paper we have discussed various pixel-based techniques for image forgery detection, mainly copy-move and splicing techniques.

Keywords:
Image forgery, Image forgery detection, Copy-move, Splicing, Tampering.

1. INTRODUCTION

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 software and editing tools, an image can be easily manipulated and modified [1]. 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 [2]. 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 [3].

The main goal of this paper is:

- to introduce various aspects of image forgery detection;
- to review some recent and existing techniques in pixel-based image forgery detection;
- to provide a comparative study of existing techniques with their pros and cons.

Digital image forgery detection techniques are classified into active and passive approaches. In the active approach, the digital image requires preprocessing of image such as watermark embedding or signature generation, which limits their application in practice [3].

Unlike the watermark and signature-based methods, the passive techniques do not need any digital signature to be generated or to embed any watermark.

Passive image forgery detection techniques roughly can be divided into five categories [4] as shown in Figure 1. Pixel-based techniques detect statistical anomalies introduced at the pixel level; format-based techniques leverage the statistical correlations introduced by a specific lossy compression scheme; camera-based techniques exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing; physical environment-based techniques explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and geometry-based techniques make measurements of objects in the world and their positions relative to the camera.

1. Pixel-based image forgery detection: Pixel-based techniques emphasize on the pixels of the digital image. These techniques are roughly categorized into four types. We are focusing only two types of techniques copy-move and splicing in this paper. This is one of the most common forgery detection techniques. Figure 2 shows categorization of pixel-based forgery detection techniques.
2. Format-based image forgery detection: Format-based techniques are another type of image forgery detection techniques. These are based on image formats and work mainly in the JPEG format. These techniques can be divided into three types (Figure 3). If the image is compressed then it is very

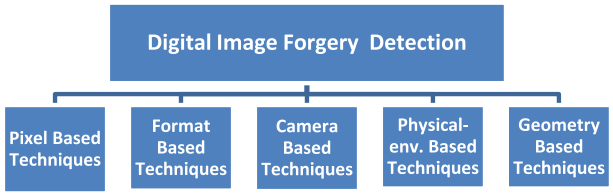

Figure 1: Digital image forgery detection techniques.

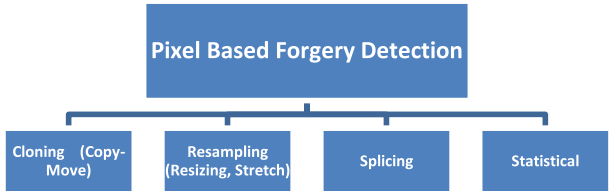

Figure 2: Pixel-based image forgery detection.

difficult to detect forgery but these techniques can detect forgery in the compressed image.

3. Camera-based image forgery detection: Whenever we capture an image from a digital camera, the image moves from the camera sensor to the memory and it undergoes a series of processing steps, including quantization, colour correlation, gamma correction, white balancing, filtering, and JPEG compression. These processing steps from capturing to saving the image in the memory may vary on the basis of camera model and camera artifacts. These techniques work on this principle. These techniques can be divided into four categories as shown in Figure 4.
4. Physical environment-based image forgery detection: Consider the creation of a forgery showing two movie stars, rumoured to be romantically involved, walking down a sunset beach. Such an image might be created by splicing together individual images of each movie star. In so doing, it is often difficult to exactly match the lighting effects under which each person was originally photographed. Differences in lighting across an image can then be used as evidence of tampering. These techniques work on the basis of the lighting environment under which an object or image is captured. Lighting is very important for capturing an image. These technique are divided into three categories as shown in Figure 5 [4].
5. Geometry-based image forgery detection: Grooves made in gun barrels impart a spin onto the projectile for increased accuracy and range. These grooves introduce somewhat distinct markings to the bullet fired, and can therefore be used to link a bullet with a specific handgun. In the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. Geometry-based techniques make measurement of objects in the world and their position relative to the camera. Geometry-based image forgery techniques are divided into two categories (Figure 6) [4].

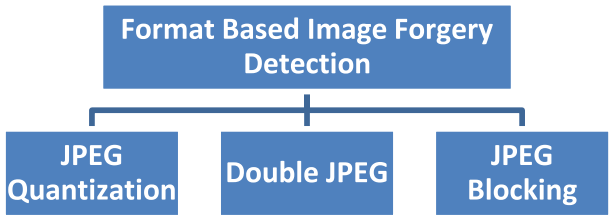

Figure 3: Format-based image forgery detection.

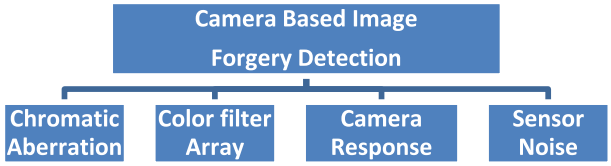

Figure 4: Camera-based image forgery detection.

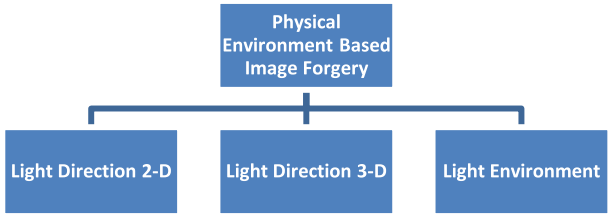

Figure 5: Physical environment-based image forgery detection.

The rest of the paper is organized as follows. In Section 2, we have described pixel-based image forgery detection. In Section 3, we present and discuss various existing techniques of pixel-based image forgery detection, mainly copy-move and splicing. In Section 4, a comparison of various algorithms is given. Section 5 provides the conclusion of this paper.

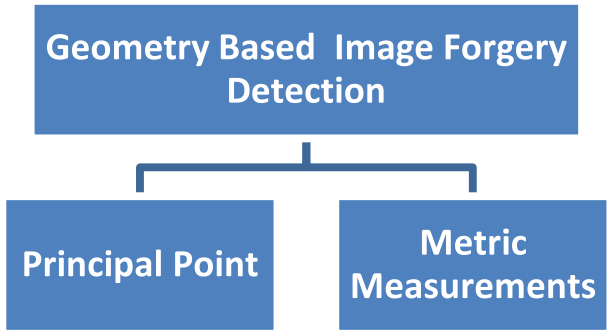

Figure 6: Geometry-based image forgery detection.

Figure 7: Original image.

2. PIXEL-BASED IMAGE FORGERY DETECTION

Pixel-based image forgery detection is roughly categorized into four categories (Figure 2). Pixel-based techniques detect statistical anomalies introduced at the pixel level [1,4].

2.1 Cloning (Copy-Move)

This is the most common type of image forgery and this is also known as copy-move forgery. In the copy-move a part of the image is copied and pasted somewhere else within the image. Figure 7 shows the original image with six balloons and Figure 8 shows the tampered image with nine balloons.

2.2 Resampling (Resize, Stretch, Rotate)

For making a composite of two people it might be possible that one person may have to be resized, stretched to match the relative height of other people. So this process needs to resample original image into a new sampling lattice [5].

Figure 8: Tampered image.

Figure 9: Image used in splicing.

Figure 10: Another image used in splicing.

2.3 Splicing

This is another type of image forgery. In this technique digital splicing of two or more images is done into a single composite image [6]. Suppose we have two images (Figures 9 and 10), both images are spliced into a single composite image (Figure 11). When performed carefully, the border between the spliced regions can be visually hardly noticeable.

3. EXISTING PIXEL-BASED IMAGE FORGERY DETECTION TECHNIQUES

There are many approaches that have been proposed by various authors for detecting pixel-based image forgery. Figure 12 shows the general process of detecting copy-move image forgery [2, 5–21].

Figure 11: Spliced image.

PCA: principal component analysis; DCT: discrete cosine transform; DWT: discrete wavelet transform; SVD: singular value decomposition; SIFT: scale invariant feature transform; SURF: speeded up robust features.

Fridrich et al. [13] proposed a method for detecting copy-move image forgery in 2003. In this method, the image is divided into overlapping blocks (16×16) for feature extraction. Authors have used DCT coefficients for feature extraction. Then, the DCT coefficients of blocks are lexicographically sorted. After lexicographical sorting, similar blocks are detected and forged regions are found. In this paper authors perform robust retouching operations in the image. But authors have not performed any other robustness test.

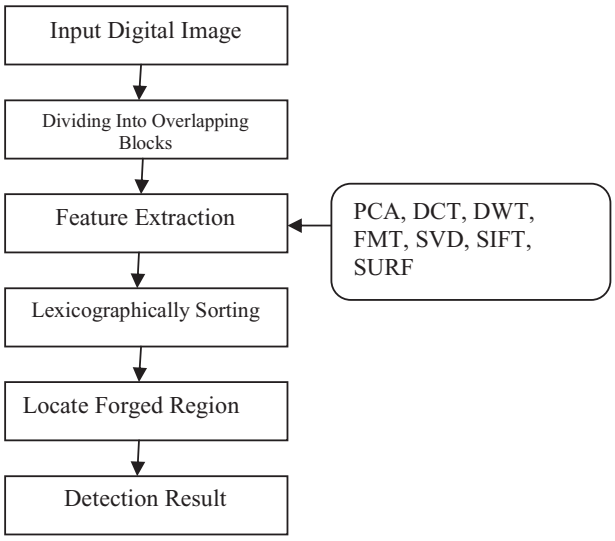

Figure 12: Block diagram of copy-move image forgery detection system.

Popescu et al. [14] proposed a technique for detecting duplicate image regions in 2004. In this paper, authors applied PCA on small fixed-size image blocks (16 × 16, 32 × 32). They computed the eigenvalues and eigenvectors of each block. After applying lexicographical sorting, the duplicate regions are automatically detected.

This algorithm is an efficient and robust technique for detecting a tampered region automatically. The advantage of this algorithm is the ability to detect duplicate region even if the image is compressed or noisy.

Kang and Wei [8] proposed the use of SVD to identify the tampered regions in a digital image in 2008. In this paper Authors used SVD for extracting feature vector and dimension reduction. Lexicographical sorting is applied on rows & column vectors and similar blocks are identified to detect forged regions. This algorithm is robust and efficient.

Lin et al. [15] proposed a fast copy-move forgery detection technique in 2009. In this paper Authors used PCA for finding features vectors and dimension reduction then Radix sort is applied on feature vectors to detect forgery. This algorithm is efficient and works well in noisy and compressed images.

Huang et al. [9] proposed the detection of copy-move forgery in digital images using SIFT algorithm in 2009. In this paper, authors introduced SIFT algorithm using feature matching. The algorithm provides good results even when image is noisy or compressed.

Li et al. [10] proposed a sorted neighbourhood approach for detecting duplicate region based on DWT and SVD in 2007. In this paper, authors used DWT and decomposed into four sub-bands. SVD was used in low-frequency sub-bands to reduce dimension representation. Then, they applied lexicographical sorting on singular value vector and the forged region is detected. They tested grey-scale and colour images for detecting duplicate region. This algorithm is robust.

Luo et al. [16] proposed a robust detection of region duplication in digital images in 2006. In this paper, authors divide an image into overlapping blocks and then apply the similarity matching on these blocks. The similarity matching identifies the duplicate regions in the image. This method also works in the JPEG compression, Gaussian blurring, and additive noise.

Zhang et al. [17] proposed a new approach for detecting copy-move forgery detection in digital images in 2008. Authors used DWT and divided low-frequency band into four non-overlapping sub-images and phase correlation is adopted to compute the spatial offset between the copy-move regions. Then, they applied pixel matching for detecting the forged region. This algorithm works well in the highly compressed image. This is a very effective algorithm with lower computational time compared with other algorithms.

Kang et al. [18] proposed copy-move forgery detection in digital image in 2010. Authors divided the image into sub-blocks and used improved SVD. Then, similarity matching is performed on the lexicographically sorted SV vectors and the forged region in the images is detected.

Ghorbani et al. [11] proposed DWT-DCT (QCD)-based copy-move image forgery detection in 2011. Authors used DWT and resolved the image into sub-bands and then performed DCT-QCD (quantization coefficient decomposition) in row vectors to reduce vector length. After lexicographically sorting the row vectors, shift vector is computed. Finally, the shift vector is compared with threshold and the forged region is highlighted.

Lin et al. [7] proposed an integrated technique for splicing and copy-move image forgery detection in 2011. First, the authors converted an image into the

Table 1: Comparative study of existing techniques.

S. No.	Paper title	Method used	Tampering detection type	Pros/cons	Publication year
1.	Detection of copy-move forgery in digital image [13]	DCT	Copy-move region is detected	Will not work in noisy image	2003
2.	Exposing digital forgeries by detecting duplicated image regions [14]	PCA	Exact copy-move region is detected automatically	Time complexity is high	2004
3.	Robust detection of region duplication in digital image [16]	Similarity matching	Copy-move region detected in noisy conditions	Time complexity is reduced [14]	2006
4.	A sorted neighbourhood approach for detecting duplicate reason based on DWT and SVD [10]	DWT-SVD	Efficiently detects forged region	Time complexity is less compared to other algorithms [14]	2007
5.	A new approach for detecting copy-move forgery detection in digital image [17]	DWT	Exact copy-move region is detected	Works well in noisy and compressed image	2008
6.	Detection of copy-move forgery in digital images using SIFT algorithm [9]	SIFT	Copy-move region is detected	Detects false result also	2008
7.	Identifying tampered regions using singular value decomposition in Digital image forensics [8]	SVD	Copy-Move region is detected accurately	Will not work in highly noised & compressed image	2008
8.	Fast copy-move forgery detection [15]	Improved PCA	Exact Copy-Move region is detected	Works well in noisy, compressed image	2009
9.	Detect digital image splicing with visual cues [6]	DW-VAM	In spliced image, forged region is detected	Work only in the Splicing	2009
10.	Fast, automatic and fine-grained tempered JPEG image detection via DCT coefficient analysis [19]	Double Quantization – DCT	Tampered region is detected accurately	Works only in JPEG Format	2009
11.	Copy-move forgery detection in digital image [18]	SVD	Forged region is detected	Will not work well in noisy image	2010
12.	DWT-DCT based Copy-Move image forgery detection [11]	DCT-DWT	Forged region is detected accurately	Will not work in highly compressed image	2011
13.	An integrated technique for splicing and copy-move image forgery detection [7]	DCT-SURF	Copy-Move and spliced both region detected	Works well for both copy-move and splicing	2011
14.	Improved DCT-based detection of copy-move forgery in digital image [22]	DCT	Copy-move region detected accurately	Works well if the image blurred & compressed	2011
15.	A robust detection algorithm for copy move forgery in a digital image [23]	DCT	Exact copy-move region detected	Works well if the image is noisy or blurred	2012

YCbCr colour space. For splicing detection, the image is divided into sub-blocks and DCT is used for feature extraction. For copy-move detection, SURF is used. The algorithm works well in both splicing and copy-move image forgery detection.

Qu et al. [6] proposed a technique to detect digital image splicing with visual cues in 2009. The authors used a detection window and divided it into nine sub-blocks. VAM (visual attention model) is used to identify a fixation point and then feature extraction for extracting the spliced region in the image.

Lin et al. [19] proposed a fast, automatic, and fine-grained tampered JPEG image detection technique using DCT coefficient analysis in 2009. Authors have used DCT coefficient and Bayesian approach for detecting a forged block. Feature extraction is applied to extract the forged region.

Huang et al. [22]. proposed Improved DCT-based copy move forgery detection in image in 2011. Authors have used DCT for finding feature vector than applied matching operations to detect forgery regions.

Cao et al. [23]. proposed a robust detection algorithm for copy-move forgery in digital image in 2012. Authors have used DCT for finding DC coefficient, each block represent by circle block and extract feature from each circle block. Searching similar block pairs and find forgery region.

4. COMPARISON

We have discussed various methods used for image forgery detection proposed by various authors. The motive of all the methods is to detect the forgery in the image but the techniques are different. Table 1 shows the comparison table of the various methods discussed in this paper.

5. CONCLUSION

In this paper various approaches of pixel-based image forgery detection have been reviewed and discussed. All the methods and approaches discussed in this paper are able to detect forgery. But some algorithms are not effective in terms of detecting actual forged region. On the other hand some algorithms have a very high time complexity. So, there is a need to develop an efficient and accurate image forgery detection algorithms.

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. 133−62, Jan. 2011.
2. J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," *Acta Automatica Sinica*, Vol. 35, no. 12, pp. 1488−95, 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. 16−25, Mar. 2009.
5. 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.
6. Z. Qu, and G. Qiu, "Detect digital image splicing with visual cues" *Lect. Notes Comput. Sci.*, Vol. 5806, pp. 247−26, Jan. 2009.
7. S. D. Lin et al., "An integrated technique for splicing and copy-move forgery image detection," in *IEEE 4th International Congress on Image and Signal Processing (CISP)*, Vol. 2, 2011, pp. 1086−90.
8. 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. 926−30.
9. 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. 272−6.
10. 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. 1750−3.
11. M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in *18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP)*, 2011, pp. 1−4.
12. I. Amerini 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. 1099−111, 2011.
13. J. Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop*, Aug. 2003, pp. 5−8.
14. A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
15. H.-J. Lin, C.-W. Wang, and Y.-T. Kao, "Fast copy-move forgery detection," in *WSEAS Transaction on Signal Processing*, 2009, pp. 188−97.
16. 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. 746−9, 2006.
17. 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. 362−6.
18. 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. 2419−21.
19. Z. Lin et al., "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", *Pattern Recogn.*, Vol. 42, pp. 2492−250, 2009.

20. X. Pan, and S. Lyu, "Region duplication detection using image feature matching," *IEEE Trans. Inf. Foren. Sec.*, Vol. 5, no. 4, pp. 857–67, Dec. 2010.
21. R. C. Gonzalez, and R. E. Woods, "Digital Image Processing Using Matlab," *Pearson Education India, 2004*.
22. Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images". *Forensic Sci. Int.* Vol. 206, pp. 178–84, 2011
23. Yanjun Cao, T. Gao, and Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images" *Forensic Int.* Vol. 214, pp. 33–43, 2012.

Authors

Mr Mohd Dilshad Ansari is pursuing his PhD degree in image processing at Jaypee University of Information Technology, Waknaghat, Solan (HP), India. He received his MTech degree in computer science and engineering in 2011. He received his BTech degree in information technology from Invertis Institute of Engineering and Technology, Bareilly, Uttar Pradesh, India, in 2009. His interests include image forensics, image processing.

E-mail: m.dilshadcse@gmail.com

Prof. Satya Prakash Ghrera is a professor and HoD of the Department of Computer Science and Engineering at Jaypee University of Information Technology, Waknaghat, Solan (HP), India. His research interests include image processing.

E-mail: sp.ghrera@juic.ac.in

Dr Vipin Tyagi, a fellow of IETE, is working as an associate professor in the Department of CSE at Jaypee University of Engineering and Technology, Raghogarh, Guna (MP). He is working in the area of image processing.

E-mail: dr.vipin.tyagi@gmail.com

DOI: 10.1080/09747338.2014.921415; Copyright © 2014 by the IETE