International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.8, No.7 (2015), pp.265-272
http://dx.doi.org/10.14257/ijsip.2015.8.7.25

Analysis of Copy-move Forgery Image Forensics: A Review

Nandini Singhal and Savita Gandhani

Banasthali University, Jaipur, India
Technocrats institute of technology, Bhopal, India
Nandini2singhal@gmail.com, mtech.it27@gmail.com

Abstract

In the era of today's world verification of images plays an important role. Various image editing tools are available in the market which can make changes in image in different ways. By using these tools, we can make slight changes in the image by resizing, rotating, noise addition and stretching an image or by splicing or copy move which is difficult to detect by human eyes. The digital images plays important role in many fields such as criminal and forensic investigation, military, journalism etc. So we needed some forgery detection technique for digital image. This paper reviews techniques for pixel-based forgery detection. First is copy-move or cloning and second is fast-copy move detection. In copy-move or cloning technique a part of the image is copied and pasted into another part of the image. But this image has limitation of only shifting of copied regions. So, second technique fast-copy move detection is discussed. Its result is complex but precise. Main disadvantage of fast-copy move technique it is not being able to detect for very small region.

Keywords: *Image forensics, pixel-based image forgery, discrete wavelet transform, phase correlation*

1. Introduction

The digital image passes through various processing steps during its life cycle. So it can be edited according to the need. Adding, deleting, resizing, rotating content of an image insist and popular way of creating image forgery. To verify the content of images we need some approaches. Research in community classified this approach into two wide areas namely as active and passive approach shown in Figure 1. In [1, 2] Active approach some information has to be kept at source side such as Digital watermark [3-5] or Digital signature [6, 7]. And later changes of the image can be detected by comparing value of the Digital watermark or Digital signature with image. But for this Active approach digital cameras should be equipped with a watermarking or Digital signature chip to store Digital signature or Digital watermark

For trustworthiness camera would require the manufacturers to define a common standard protocol. This requirement of cameras is too hard to satisfy. This would constraint the application of such solution only to very limited scenarios. To overcome this problem, a method for authenticating the content of images has evolved, that doesn't need any prior information about the image, defined as Passive approach [8-10].

.

ISSN: 2005-4254 IJSIP

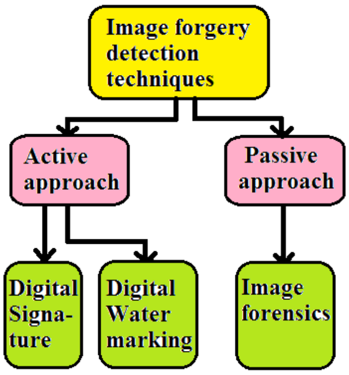


Figure 1. Image Forgery Detection Techniques

Image forensic is a passive approach that studies the use of scientific methods for gaining probative facts from digital evidences. The task of image forensic tools is to expose the traces left in image content by each steps of its life, exploring existing knowledge on digital imaging research. The research activity in Image forensics started few years ago and increased very much in the last few months. These passive approach works without the presence of Digital signature or Digital watermark. These approaches work when a digital forgery doesn't leave any visual clues that indicate any tempering, but they may alter some important content of image.

Researchers have classified these image forensic tools into five categories

- Pixel-based approach that works at pixel level.
- Format-based approach that are based on image formats and work mainly for the JPEG format.
- Camera-based image forgery approach during capturing of an image from a digital camera, the images move from camera sensor to the memory by series of processing steps. These steps can vary on the camera model.
- Physically-based approach works to detect anomalies in 3-D interaction between physical objects, light and the camera.
- Geometric based approach make measurement of objects in the world and their position relative to the camera.

2. Literature Review

There are many approaches that have been proposed by various authors for detecting image forgery. In [11], major processing stages inside the camera are discussed. This paper also reviews several methods for source digital camera identification and forgery detection. Existing methods for source identification explore the various processing stage inside a camera to derive the clues for distinguishing the source cameras while forgery detection checks for inconsistencies in image quality

In [12], problem of detecting copy-move forgery is discussed. And they describe an efficient and reliable detection method. This method may successfully detect the forged part even when the copied area is altered to merge it with the background and when the forged image is saved in a lossy format.

In [13], researcher focuses on methods to detect digital forgeries created from multiple images called as copy-create image forgeries.

In [14], image forensic tools have been reviewed by classifying them according to the position in the history of the image in which the relative footprint is left. Two approaches for image forensic are discussed namely as Active approach and Passive approach.

In [15], different techniques for copy move forgery is discussed. There are five types of image forgery techniques under passive approach. 1. Pixel-based detection technique. 2.

Format-based detection technique. 3. Physics-based detection technique. 4. Geometric-based detection technique. 5. Camera-based detection technique.

In [16], non-intrusive methods are discussed which help in dealing with copy-move forgery. Block matching is one of the most frequently used non-intrusive approaches for copy-move forgery detection.

In [17], a parallel algorithm for the copy-move forgery detection is discussed, which help in decreasing execution time of the algorithm. The method uses overlapping blocks and lexicographical sorting in a parallel manner.

In [18], a method called fast-copy move forgery detection is discussed. In this method the given image is divided into overlapping blocks of equal size, feature for each block is then extracted as a vector; all the extracted feature vectors are then sorted using the radix sort. Radix sort dramatically improves the time complexity and the adopted features enhance the capability of resisting of various attackers such as JPEG compression and Gaussian noise.

In [19], a pixel-based image forgery detection technique is discussed. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. This paper reviews way for tampering an image such as splicing or copy-move re-sampling an image (resize, rotate), addition, removal of any object from the image.

3. Current Techniques

Researcher has classified five categories for image forgery detection under passive approach:

1) Pixel-based approach
2) Format-based approach
3) Camera-based image forgery approach
4) Physically-based approach
5) Geometric based approach.

From the above five categories, we are focusing on Pixel-based forgery detection techniques. There are four techniques under Pixel-based category namely as copy-move (Cloning), fast-copy detection (Splicing), statistical, re-sampling. Figure 2 shows the categorization of pixel-based forgery detection technique.

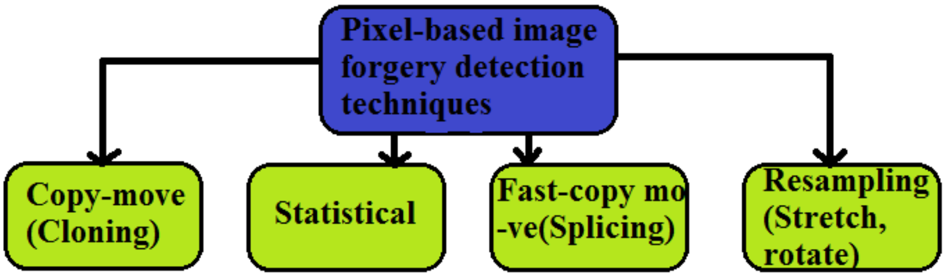

Pixel-based image forgery detection techniques
Copy-move (Cloning)
Statistical
Fast-copy mo -ve(Splicing)
Resampling (Stretch, rotate)

Figure 2. Pixel-based Image Forgery Detection Techniques

Pixel-based approach mainly focuses on the pixels of the image. From four categories we are focusing on one category, *i.e.*, copy-move forgery detection. This is most common tampering technique. All techniques are defined as follows.

A. Re-sampling

In re-sampling, we resize, rotate and stretch the digital image. For ex. to make a composite of two people it might be possible that one person may have to be stretched, resized to match the relative height of other person. So this requires re-sampling original image into a new sampling lattice.

B. Statistical

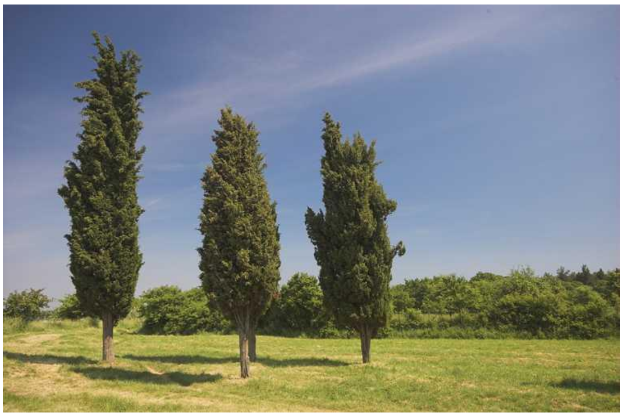
This is another important image forgery detection technique under pixel-based forgery detection category. There are total number of 256^{n^2} possible 8-bit grayscale images of size n×n. with as few as n=10 pixels, there are a whopping 10^{240} possible images. If we were to randomly draw from this space of possible images, it would be exceedingly to obtain a perceptually meaningful image. These observations suggest that photographs contain specific statistical properties. In papers [20-22] author has exploited statistical regularities in natural images to detect various types of manipulations.

C. Fast-copy move forgery detection technique

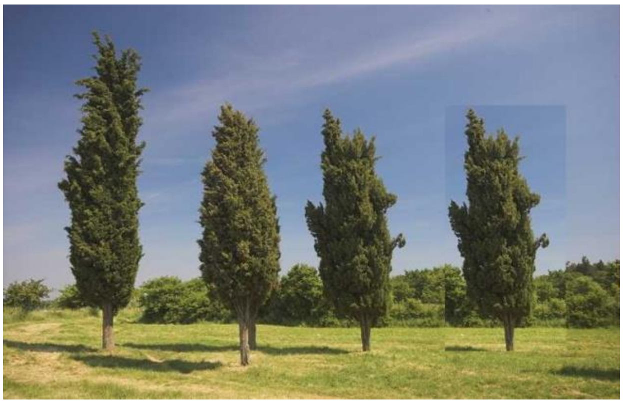
The authors in [18], proposed a method for detecting copy-move forgery over images altered by copy-move. This forgery technique first divided image into overlapping blocks of equal size, feature for each block is then extracted and represented as a vector. All the extracted vectors are then sorted using radix sort. In sorting compute the difference of the position of every pair of adjacent feature vectors. The accumulated number of each of the shift vectors is evaluated.

D. Copy-move forgery detection technique

This is one of the difficult forgeries and used where one needs to cover a part of the image in order to add or remove information. In this manipulation technique a part of the image is copied and pasted into another part of the same image. By pasting a part of image to another part of image it can hide important information or object from the image. For this type of pasting in an image, where editing cannot be detected by human eyes, copy-move forgery is used for authenticity of that image. This technique introduces a correlation between the original image area and the pasted content. Resizing, rotating of pasted portion of an image is also necessary to create a convincing forgery. Figure 3 shows an example of copy–move forgery: A) Original image with three trees and B) The forged image with four trees.



A)



B)

Figure 3. An Example of Copy–move Forgery: A) Original Image with Three Trees and B) The Forged Image with Four Trees

Algorithm for copy-move forgery detection
Step 1: Apply DWT to the input image to yield LL1 sub-band.
Step 2: Divide the LL1 sub-band into sub-images.
Step 3: Calculate phase correlation
Step 4: Calculate the offset between the copy-move regions
Step 5: Find out the copy-move region by pixel matching.
Step 6: Apply MMO (Mathematical Morphological Operations)
Step 7: Detect the result

Figure 4 shows flow chart of copy-move forgery algorithm

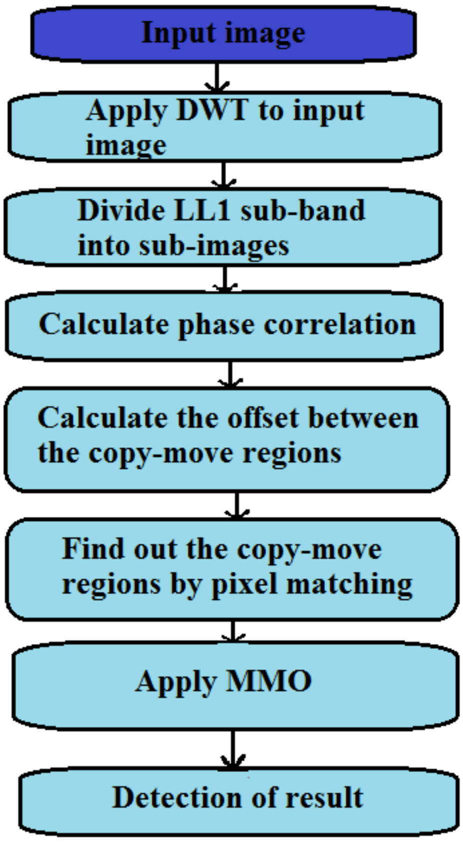

Input image
Apply DWT to input image
Divide LL1 sub-band into sub-images
Calculate phase correlation
Calculate the offset between the copy-move regions
Find out the copy-move regions by pixel matching
Apply MMO
Detection of result

Figure 4. Flow Chart of Copy-move Forgery

DWT is applied to the input image to yield a reduce dimension called LL1 sub-band (Four sub-bans are output). This is a multilevel decomposition technique, is localized in space and in frequency. The localization feature leads to a number of useful applications such as data compression, detecting features in images and removing noise and so on [12]. The author has performed Haar wavelet to reduce the dimension of the image, and then four sub-bands are output. As the low frequency sub-band concentrates most of the image energy, whose size is only $1/4^l$ of the original image, where 'l' is a positive integer. As a result, the size of a forged $M \times N$ image is reduced to $M \times N/4^l$.

To detect duplicate regions in an image, comparison of every pair of region is required, because the regions are in different shape and size. Most of the overlapping blocks methods [23-27], divide the image into $k \times k$ pixels fixed-sized overlapping blocks. Blocks are slid by one pixel along the image from the upper left corner right down to the lower right corner. For $M \times N$ pixels image, the sliding will generate $(M-k+1) \times (N-k+1)$ such blocks. As the size of the forged image is reduced to$M \times N/4^l$, the approach will generate p blocks where$p = \left(\frac{M}{2^l} - k + 1\right) \times (\frac{N}{2^l} - k + 1) \approx M \times N/4^l$.

We have an image R (m, n) by shifting ($\triangle m, \triangle n$), we can get the image R'(m,n), such that

$$\boldsymbol{R'(m,n) = R(m - \triangle m, n - \triangle n)} \qquad \textbf{(1)}$$

Fourier transform of R (m, n) and R' (m, n) are F(u, v) and F'(u, v) respectively.

$$\boldsymbol{F'(u,v) = F(u,v)e^{-ju\triangle m + v\triangle n}} \qquad \textbf{(2)}$$

The normalized cross power spectrum of F(u, v) and F'(u, v) is given by:

$$\mathbf{P(u,\ v) = F}\frac{\boldsymbol{(u,v)F'^{*}(u,v)}}{\boldsymbol{|F(u,v)F'^{*}(u,v)|}}$$

$$\boldsymbol{= e^{ju\triangle m + v\triangle n}} \qquad \textbf{(3)}$$

Where,
* → Complex conjugate
||.|| → Complex magnitude

Let the image inverse Fourier transform of P(u, v) is P(m, n). Phase correlation techniques estimate spatial offsets by extracting peaks in P(m, n). The spatial location of a peak corresponds to the spatial offset ($\triangle m, \triangle n$).

To locate copy-move region by pixel-matching, each pair of sub-blocks is tested whether they are similar. As an example of copy-move forgery Figure 5 shows R(m, n), where m and n are top left corner co-ordinate of the corresponding block is copied and pasted as the region R'(m, n) in the same image.

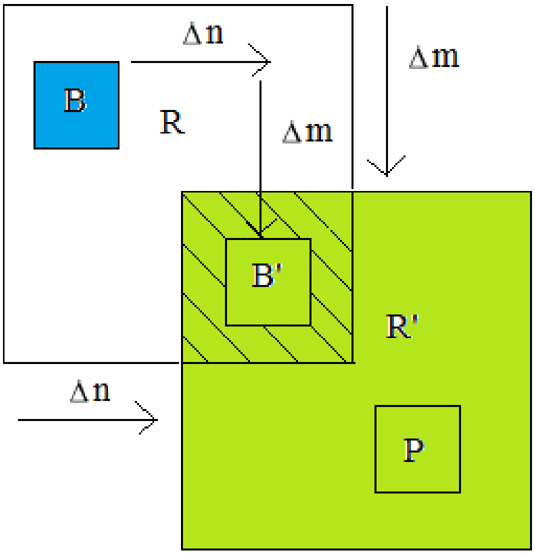


Figure 5. Pixel-matching by Image Shifting

The distance between the original and the pasted region is,

$$\boldsymbol{d} = (\triangle \boldsymbol{m}, \triangle \boldsymbol{n})$$

Notation used,
R → Original image
R' → Duplicate image
B → Original block in region R
B' → Pasted block in region R'
P → Pasted part of image

Therefore, these pairs of original and pasted blocks (B, B') can be confirmed as duplication forgery without further testing. Such blocks are called UTO (Unnecessary Testing Blocks). Main advantage of this approach is that we can skip as much as possible UTB in the copy-move regions [28].

Let us assume the overlaid part in R' (m, n) asR'_f, the corresponding part in the shifted version asR_f, i.e., R_f is shifted to $R'_f$by $(\triangle m, \triangle n)$.

If (m, n) is does not belongs to R_f

$$R_{\triangle}(m,n) = R'(m,n)$$

If (m, n) belongs to R_f

$$R_{\triangle}(m,n) = 0$$

Else

$$R_{\triangle}(m,n) = |R'(m + \triangle m, n + \triangle n) - R'(m,n)|$$

4. Conclusion

In this paper a special type of forgery detection is discussed, which can detect the duplicated regions accurately and quickly. The efficiency of forgery detection can improve by applying DWT (Discrete Wavelet Transform).

References

[1] G. L. Friedman, "Trustworthy digital camera: restoring credibility to the photographic image," IEEE Transactions on Consumer Electronics, vol. 39, no. 4, (**1993**), pp. 905–910.

[2] P. Blythe and J. Fridrich, "Secure digital camera," in Proceedings of the Digital Forensic Research Workshop (DFRWS '04), (**2004**), pp. 17–19.

[3] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking, Morgan Kaufmann, (**2001**).

[4] M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications, Signal Processing and Communications, Marcel Dekker, (**2004**).

[5] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, 'Digital Water—Marking and Steganography", Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition, (**2008**).

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, (**1978**), pp. 120–126.

[7] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, "Handbook of Applied Cryptography", CRC Press, Boca Raton, Fla, USA, 1st edition, (**1996**).

[8] H. Farid, "Image forgery detection," IEEE Signal Processing Magazine, vol. 26, no. 2, (**2009**), pp. 16–25.

[9] T. Van Lanh, K. S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A survey on digital camera image forensic methods", in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07), (**2007**) July, pp. 16–19.

[10] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Signal Processing: Image Communication, vol. 25, no. 6, (**2010**), pp. 389–399.

[11] T. V. Lanh, K.-S. Chong, S. Emmanuel and M. S. Kankanhalli, "A SURVEY ON DIGITAL CAMERA IMAGE FORENSIC METHODS", in ICME (**2007**).

[12] P. Deshpande and P. Kanikar, "Pixel Based Digital Image Forgery Detection Techniques", International Journal of Engineering Research and Applications (IJERA) vol. 2, no. 3, (**2012**) May-June, pp. 539-543 539.

[13] S. Murali, G. B. Chittapur, P. H. S and B. S. Anami, "COMPARISON AND ANALYSIS OF PHOTO IMAGE FORGERY DETECTION TECHNIQUES" International Journal on Computational Sciences & Applications (IJCSA) vol. 2, no. 6, (**2012**) December.

[14] A. Piva, "An Overview on Image Forensics", Hindawi Publishing Corporation ISRN Signal Processing vol. 2013, Article ID 496701, 22 pages.

[15] S. Alam and D. Ojha, "A Literature study on Image forgery", International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 10, (**2014**) October.

[16] N. Muhammad, M. Hussain, G. Muhamad, and G. Bebis, "A Non-intrusive Method for Copy-Move Forgery Detection", G. Bebis et al. (Eds.): ISVC 2011, Part II, LNCS 6939, (**2011**), pp. 516–525.

[17] M. Sridevi, C. Mala and S. Sandeep, "COPY – MOVE IMAGE FORGERY DETECTION IN A PARALLEL ENVIRONMENT", Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, (**2012**), pp. 19–29.

[18] H.-J. Lin, C.-W. Wang and Y.-T. Kao, "Fast Copy-Move Forgery Detection", ISSN: 1790-5052 189, vol. 5, no. 5, (**2009**) May.

[19] M. D. Ansaria, S. P. Ghreraa and V. Tyagi, "Pixel-Based Image Forgery Detection: A Review", IETE Journal of Education.

[20] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection with binary similarity measures", In European Signal Processing Conference, Turkey, (**2005**).

[21] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection", Journal of Electronic Imaging, vol. 15, no. 4, 041102, (**2006**).

[22] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics", In IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), Madison, Wisconsin, (**2003**).

[23] J. Fridrich, D. Soukal and J. Lukáš, "Detection of copy-move forgery in digital images", In Proc. Digital Forensic Res. Workshop. Cleveland (USA), (**2003**) August.

[24] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling", IEEE Transactions on Signal Processing, vol. 53, no. 10, (**2005)** pp. 758-767.

[25] S. Bayram, H. T. Sencar and N. Memon, "An efficient and robust method for detecting copy-move forgery", In IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP 2009, (**2009**), pp.1053-1056.

[26] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", Forensic Science International, vol. 171, no. 2, (**2007**), p. 180-189.

[27] Y. Huang, W. Lu, W. Sun and D. Long, "Improved DCT-based detection of copy-move forgery in images", Forensic Science International, vol. 206, no. 1-3, (**2011**), p. 178-184.

[28] B. Yang, X. Sun, X. Chen, J. Zhang and X. Li, "An Efficient Forensic Method for Copy–move Forgery Detection Based on DWT-FWHT", RADIOENGINEERING, vol. 22, no. 4, (**2013**) December.