Cloned Image Forgery Detection- A Review

Swati Mehta[1] Garima Goel[2]
[1,2]Department of Computer Science
[1,2]Kurukshetra University Kurukshetra, India

Abstract—In today's era role of digital image is eloquent. With its escalating importance and usage it becomes necessary to assess if the content is realistic or has been manipulated to trick the observer. Image forensics answers all these questions. Adding some useful features or eliminating awkward information is the extensively used tampering technique. The image forgery caused using this technique refers to cloning or copy-move attack. This paper elaborates the manifold techniques to detect cloned image forgery.

Key words: Cloning, Copy-Move Attack, Image Forgery, Image Forensics, Tampering

I. Introduction

Considerable amount of information is portrayed from images stored digitally. But today we cannot completely rely on data extracted from an image because due to availability of massive elementary softwares images can be comfortably molded. Precedent to confiding with an image's data should be carefully tested. Image Forensics [1] specifies tactics that are employed to legitimize the truthfulness of an image. Pertinence of Digital Image Forensics can never be overlooked in today's era [2]. Digital Image Forgery provides diversified methods to uncover any type of fabrication. These methods are first categorized as: active and passive [3]. The former approach requiring some pre-processing like watermarking, signature, etc. is active one. Passive one does not require any watermark to be embedded.

Digital Watermarking [4] is an active approach whereas Copy-move forgery [5] belongs to passive or blind approach. The main flaw of active approach is that it requires embedding of information during creation or former to its broadcast to public. Cloning attack refers to copying and pasting chunks of an image to forge an object or obscure a person in a scene. There are numerous algorithms and methods accessible to detect cloning in images. This paper describes few of the customarily applied techniques for extraction of features and hence for detecting forgery- Principal Constant Analysis (PCA), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Scale Invariant Transform (SIFT).

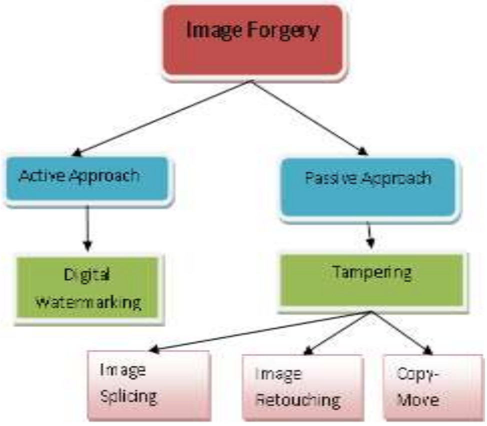


Fig. 1: Approaches to Image Forgery Detection

This paper focuses on providing a deep review on cloning forgery and discusses the various ways to uncover this genre of forgery. The variant methods that exist for disclosing copy move forgery have their own significance. DCT, DWT, PCA schemes are techniques for successful extraction of stable feature sets of an image. All of mentioned schemes have caliber of their own. The utilization of these schemes depends on the genre of problem and also on the researcher. Disparate authors have used distinct schemes and have also added their flavor to form a new strategy. The implementation of each of the technique varies a bit. The fundamental idea behind each of the scheme is somewhat similar. The suspected image is fragmented into fixed sized block. Disparate authors fragment the suspected image into fragments of size based on their research requirements.

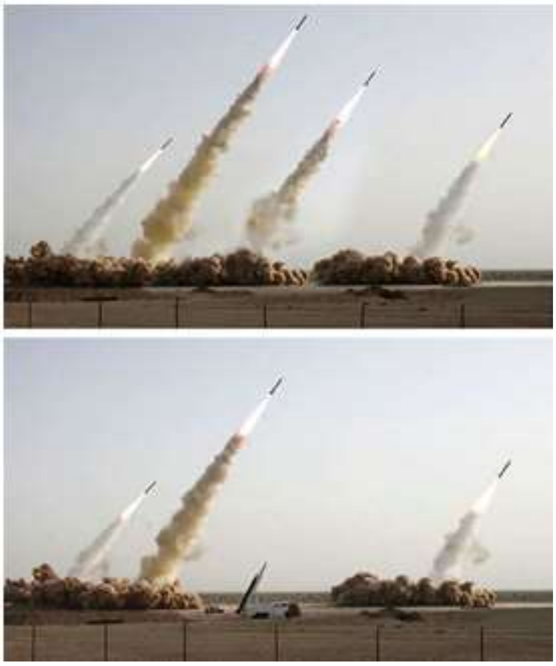


Fig. 2: Cloned image (top) : Original image(bottom)

II. Cloned Image Forgery Detection Techniques

The foremost objective of cloned image forgery detection is to uncover tampered [6] image parts. One straightforward technique to accomplish this task is exhaustive search. This process involves image comparison with its own cycle-shifted version. It is an uneconomical approach and can take $(ST)^2$ steps for size S x T. This technique fails if manipulated chunks are further modified. Another approach is unfolded for images that comprise of larger duplicated areas by Fridrich et al. [7].

The most extensively used third approach is block matching process. This formation involves fragmentation of image into its corresponding overlapping blocks. Contrary to detection of whole duplicated region the aim is to uncover connected blocks that are copied and displaced.

A firm and robust portrayal of image blocks is significant so that the molded blocks can be uncovered under modifications. To represent image blocks various authors contemplated use of numerous features. After division of image into chunks or blocks next important task is to extract essential features that yields analogous values for forged blocks, even if they are modified.

A. PCA

Popescu et al.[8] devised a technique for detection of cloned regions in an image. The researchers practiced PCA for coefficient extraction. PCA is exercised on an image smaller in size. Each block was portrayed as 16x16 and the coefficients in each block were vectorized and infused in a matrix and the corresponding covariance matrix was formed. A new linear basis was obtained by computing the Eigen vectors of the covariance matrix,

Duplicated chunks are then detected by lexicographically sorting all of the image blocks. Their method was robust to compression up to JPEG quality. This algorithm is quite competent and robust in tampered regions detection. The fundamental leverage of PCA is its capability to uncover duplicate regions even if the image is compressed or noisy.

B. DCT

PCA uncovers the duplicated regions for jpeg images but less efficiently [9]. So, another approach DCT was utilized. DCT efficiently uncovers forged chunks from jpeg images. In [10] Maind et al. elaborated this technique.

The steps involved their proposed methods were:

1) The suspected image is fragmented into fixed size blocks.
2) To generate the quantized coefficients DCT is applied to each block.
3) Each quantized block is represented by a circle block and appropriate features are extracted.
4) Similar block pairs are found.
5) Finding correct blocks and output them.

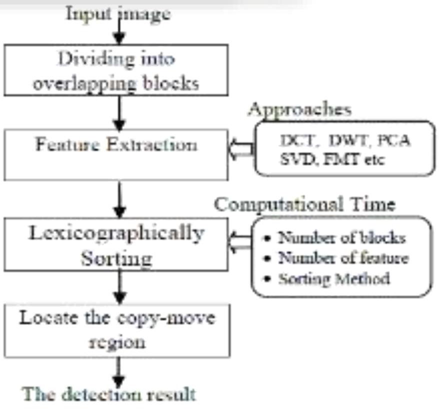


Fig. 3: Detection algorithm

DCT is not much robust when modifications are performed on input images like rotation, scaling, etc. It produces correct results when rotation is up to 5 degree.

C. SIFT

PCA and DCT are block based feature extraction technique. And for images that involve rotation and scaling of chunks these block based techniques cannot be used to produce effective results. Hence a new method SIFT is involved for feature extraction which is keypoint based technique [11].

A keypoint is a location bearing specific recognizable data of image content. Keypoint based extraction process involves uncovering image keypoints and aggregating features. SIFT method is used because it is not vulnerable to scaling, rotation and affine transformations.

The process is explained by Pan et al. in [12].

The first step is to convert the RGB image to gray scale by employing standard conversions. Distinct locations should be represented by good keypoints and features. A competent algorithm is used for keypoint extraction SIFT algorithm [13]. Stable local extrema locations in the scale space are searched to find out SIFT keypoints. A 128-dimensional vector of features is created at each keypoint. The histogram of local gradients is used for this purpose. To assure that the features extracted are unfluctuating to transformations, scaling and rotations dominant scale of the keypoint specifies the size of neighborhood.

After uncovering the keypoints they are now matched using appropriate algorithms. Next step is to evaluate possible geometric distortions of duplicated regions from the matching keypoints. It is crucial to expose all genres of potential transformations that exist between the molded regions and the pioneer image. Sometimes there occur cases when original regions and the molded regions of image are coincident. There exists a common shift vector among the pixels of molded and original image regions. In this case the distance between pair of matched SIFT keypoints is computed. And then a histogram is constructed.

If there exists scaling in an image this means molded regions are scaled before being infused into the given image. In such scenario, for all keypoint pairs the pair wise distance is enumerated to figure out the scaling constants. Then histogram of the ratios of such distance between corresponding pairs is developed. The ratio with the maximum frequency is used as an estimation of the scale factor. If a rotation transform prevails in molded image then estimation of transform cannot be done directly. Local coordinate system each for pioneer image and molded image respectively are employed and transformation between these systems is evaluated.

Now identical regions are found out by comparing every pixel with its transformation. Last step is to locate the duplicated regions by following steps described in [13].

III. SIFT AND DCT FUSED TOGETHER

DCT works well for images without geometrical transformations. The forgery detection for images that encompass rotation or scaling is somewhat problematic. SIFT works well with images that are infused with transformations. But performance of SIFT deteriorates when Gaussian noise is present. To gain worth of both the methods authors fused these schemes together.

The authors in [14] enforced both of these techniques to get better results. Two recognizable feature sets are extracted using keypoint based as well as block based schemes. The feature set derived from DCT are undeviating from Gaussian noise and JPEG compression whereas the set derived from SIFT are unfluctuating even under any type of transformation. DCT is efficient in presence of noise or any compression because of its property of strong energy compaction.

The feature set derived from SIFT are unaffected from any genre of rotation or scaling because of the fact that for each keypoint derived orientation is assigned to it. The foremost step is to uncover all the relevant keypoints and then allocate them with local descriptors. These allocated descriptors are fingerprints to keypoints. These fingerprints matching occurs utilizing relevant and appropriate algorithm like best bin first.

The author in [14] implemented the devised method on each type of image. The scheme proposed when experimented on images including rotation and scaling, for this image DCT failed but SIFT produced results efficiently. Similarly when manipulated image had additive noise in this case SIFT will not produce results but DCT will. So, in any case the devised methodology will detect the forged regions.

The basic idea behind combining was to:

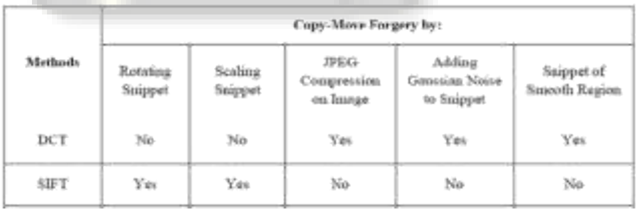
1) Take leverage of both the techniques- DCT and SIFT.
2) Devise a methodology that no more fails if noise is present or geometric transformations are applied.
3) Detect forgery even if post-processing operations are performed.
4) Produce better results in less time and within minimal cost.

The method proposed by the author works only on post-processing operations like rotation, Gaussian noise, scaling and compression.

More research is to be carried on to successfully detect forgery for other post-processing operations.

IV. COMPARISON BETWEEN DCT AND SIFT

Amanpreet Kaur and Richa Sharma effectively compared these two methods of feature extraction in [14]. They conducted various experiments on images to find out which feature extraction technique is better under which situation- DCT or SIFT.



Methods	Copy-Move Forgery by:				
	Rotating Snippet	Scaling Snippet	JPEG Compression on Image	Adding Gaussian Noise to Snippet	Snippet of Smooth Region
DCT	No	No	Yes	Yes	Yes
SIFT	Yes	Yes	No	No	No

Table 1: Comparison between DCT and SIFT

V. CONCLUSION

Image forgery by cloning attack or copy move attack is most extensively found nowadays. Numerous methods are employed by various authors to detect this forgery. This paper gives a review of various techniques that are efficiently used to extract robust feature set. All the methods are equally implemented but their implementation areas are different. Depending on the requirements any of the methods can be utilized.

REFERENCES

[1] H.Farid, “A Survey of image forgery detection”, IEEE Signal Processing Magazine, Vol. pp. 16-25, 2009.

[2] Judith A. Redi,Wiem Taktak, Jean-Luc Dugelay “Digital image forensics: a booklet for beginners” Multimedia Tools and Applications, vol. 51, no. 1, pp. 133-12, 2011.

[3] B.L.Shivakumar and S.Santhosh Baboo, “Digital Image Forgery Detection”, SAJOSPS, Vol. 10(2), pp. 116-119, 2010

[4] S.Katzenbeisser, F.Petitcolas, “Information Hiding: Techniques for Steganography and Digital Watermarking”, Artech House, 2000.

[5] B.L.Shivakumar and S.Santhosh Baboo, “Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods’, Vol. 10 Issue 7, pp. 61-65 September 2010.

[6] Sencar H. T. Memon N. Sutcu Y., Coskun B., “Tamper detection based on regularity of wavelet transform coefficients,” Proc. ICIP, International Conference on Image Processing, 2007.

[7] J. Fridrich, D. Soukal, and J. Luk, “Detection of copymove forgery in digital images,” Proc. Digital Forensic Research Workshop, Cleveland, OH, August 2003.

[8] A.C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Technical Report, TR2004-515, Dartmouth College, Computer Science, 2004.

[9] Ashima Gupta, Nisheeth Saxena, S.K. Vasistha, “Detecting copy move forgery using DCT”, Vol. 3 Issue 5, International Journal of Scientific and Research Publications, May 2013.

[10] Rohini.A.Maind, Alka Khade, D.K.Chitre,“Image Copy Move Forgery Detection using Block Representing Method”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-2, May 2014

[11] H. Huang, W. Guo, and Y. Zhang. Detection of copy-move forgery in digital images using SIFT algorithm. In IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008.

[12] Xunyu Pan, Siwei Lyu, “Region Duplication Detection Using Image Feature Matching”, IEEE Transactions On Information Forensics and Security, Vol. 5, No. 4, pp. 857-867, Dec 2010.

[13] D. Lowe, “Distinctive image features from scale-invariant keypoints,” Int. J. Comput. Vision, vol. 60, no. 2, pp. 91–110, 2004.

[14] Amanpreet Kaur and Richa Sharma, “ Copy-Move Forgery Detection using DCT and SIFT”, International Journal of Computer Applications, Volume 70– No.7, May 2013