ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

A Review on Image Forgery Detection Techniques on Passive attacks

[1] Jitesh Kumar Bhatia, [2] Anand Singh Jalal
[1][2] GLA University, Mathura, India

Abstract - **In the today's era, nearly all of us rely on the images of the memories of our lives and loved ones. The images are useful in proving anything in the court of law by showing them as an evidence of the event, getting insurance of a mishappening, getting appreciation, or for conveying personal lifestyle to their friends through social media. However, various Image editing tools like Adobe Photoshop, Picasa, and Lightroom, etc. can produce forged images, thus changing the perspective of the viewer about the event. Image Forgery has become much prominent nowadays and is being done either for fun or for an intention. Many researchers have worked in finding techniques that can classify the forged and authentic images. This objective of this paper is to provide a glimpse of work done so far in the field of Image Forgery detection.**

Keywords— Image Forensics, Image Forgery Detection Techniques, Passive Techniques, Blind Techniques.

I. INTRODUCTION

The technology has seen a progressive path of the various image and video editing tools and advancement of digital camera that has made the people doubt the authenticity of the digital images. The art of forging an image is not a new act [1]. However, in the current digital world, it is possible to create, alter and modify the content of image or video very quickly without leaving any noticeable traces of these tampering operations [1] [2]. However, due to the usefulness of the digital images in the court of law and for showing as an evidence of an event that happened in the past, the need for automatic forensic algorithms has arisen in order to find the trustworthiness of the image or the video shown for a specific purpose [3].

A. Attacks in Image Tampering

The tampering done on an original image, thus, producing a false image showing different perspective is termed as Image Forgery. According to Farid [2], the image forgery can be categorized into three major categories:

•Cloning or Copy Move: One of the most prominently used tampering attacks is Copy move. In this, the attacker performs cloning or Copy-move on an image to hide or reveal any or some part of an image. Copy move Forgery, done with an intention, is near to impossible to detect through the naked eye. However, it can be verified through some algorithms as the original pixel alignment is altered in the tampered image and can be used as a hint to identify a forgery in the image.

•Splicing: When an image is created by combining two or multiple images thus producing an image [4] the attacker wants to show to the users to change their perspective about the scene, the forgery is classified as splicing. However, though difficult to identify splicing visually, it can be identified by various factors such as the difference in noise levels, or the difference in the number of compressions in different parts of the image, etc. to name a few.

•Re-sampling: Re-sampling in an image refers to resizing, stretching, or rotation done in an image or a part of an image in order to produce a composite image having similar features. This can be used to show something that really does not exist such as person holding a pet of enormous size though the pet originally would have been comparatively smaller.

(a)

(b)

(c)

(d)

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

(e)

(f)

Fig. 1. (a) Original Image[5] (b) Forged Image after Copy Move (c,d) Original Images used for Splicing (e) Hou's Spliced Image using c and d (f) Re-sampled image

B. Classification: Image Forgery Techniques

Image Forgery Technique can be defined as a technique that can distinguish a forged Image from a set of authentic images or vice versa. The Image Forgery Detection Techniques can be classified into two parts:

•Active Authentication Techniques: In Active authentication techniques, some prior knowledge of the original image is required by the classifier. Digital watermarking and Digital signatures come under this umbrella. However, when the original image is not available, this technique cannot be carried out.

•Passive Authentication Techniques: In Passive authentication techniques, there is no need to have the original/base image. These techniques use the fact(s) that the forged image, though could not be identified through the naked eye, leaves some traces of hints behind like double compression, inconsistencies in noise, color filter, etc. to name a few. The image can be classified as forged or authentic with identification through these features.

II. LITERATURE REVIEW

A lot of work has been carried out so far to develop a classifier that can identify the given image as authentic or forged one that has undertaken the cloning attack.

A. JPEG Compression Properties

JPEG (Joint Photography Experts Group) is one of the widely accepted methods for lossy compression used for digital images. The characteristics shown by an image after JPEG compression can be utilized in an effective manner for identification of forgery in the image. An image is compressed each time an image is manipulated. Thus, the properties that occur due to double JPEG compression lead to a probability of recompression performed on the image. Ultimately, the coefficients of doubly quantized Discrete Cosine Transform show patterns repeating periodically, which acts as a clue of forgery in the image under consideration.

These effects of recompression are as shown in figure 2. The properties are showing periodic behavior which indicates that there exists double compression in the image. If we apply Fourier transform on the suspicious image, it detects that the image has been manipulated. However, the drawback of this technique is that the results are more accurate if the quality of consecutive compression is large, i.e. the later compression is done with quality lower than the quality in the former compression [6].

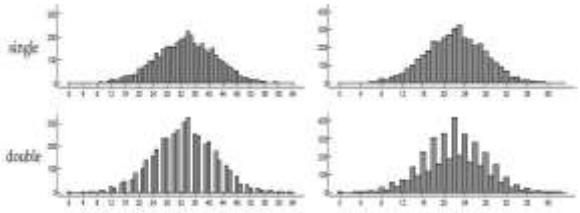


Fig. 2: Histograms (a) and (b) of images having quantization of common signal using steps 2 and 3. Histograms (c) and (d) of images having double quantization of common signal with hin respectvely. [6]

B. Detecting Traces of Resampling

Some of the image forgeries are the ones which include the composition of the images prepared after applying resizing or rotation operation(s) so that there is a convincing match between the images that have been merged together. It is done by re-sampling the host image onto a new sampling lattice. However, it produces certain specific correlations, whose detection indicates a sign of forged region in the host image.

A re-sampled signal is a combination of various samples where each sample can be expressed as the sum of approximations of its neighboring samples. After computation of the correlations between the samples, the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

expectation maximization (EM) algorithm [7] is applied. It results in the detection of the manipulation(s) done in parts of the host image. This technique is successful for a large range of manipulations, however, is only applicable for the images which undergo less compression such as JPEG, GIF, TIFF, etc. to name a few. Figure 3 shows two images on the left, the original image and the image up sampled by 10%. The corresponding figures show the magnitude of Fourier transform of probability maps as obtained by EM. It is seen that the periodic pattern is exhibited by the Fourier transforms of re-sampled signals only.

Fig. 3: Original and 10% sampled image (left) and corresponding Fourier Transform of Probability Map after applying EM algorithm (right) [7]

C. Lightning inconsistencies in Image

This category of image forgery consists of merging parts of different images to form a single image. To detect the forgery in these types of images, we need to identify the discrepancies in the parts of the image. One of the features that cause discrepancies is lightning properties in the image. In an authentic image, the lightning directions in different parts of an image are consistent [8]. Besides, the lightning condition such as the direction of light, illumination, etc. is/are inconsistent in parts of the image. This inconsistency is a hint that the image has been manipulated and is a forged image. This fact is based on the idea that the lightning directions are different in different images but same throughout an image.

For a composite image, though the forgery may not be seen through the naked eye, however, the lightning conditions remain mismatched and these act as a sign of forgery in the image under consideration. One of the drawbacks of this technique is the assumption that there is a point source of light during the capturing of the image in the image environment. Thus, the complex lightning environment may give false results [8].

Figure 4 shows a composite image that has been developed by combining the images of two stars photographed with different lightning conditions [8].

Fig. 4: A composite image where the actress' image was independently captured with non-directional source of light, whereas the actor's photograph was captured with a directional source of light kept to his left [8]

D. Exposing Image Forgery using Chromatic Aberration

Chromatic Aberration is defined as an effect that results from dispersion due to the failure of a lens to focus all the colors to the same point of convergence [9]. It is due to the fact that a lens has different refractive indices for light having different wavelengths. It leads to contraction or expansion of channels. For an image, the aberration must show consistent behavior throughout the image. In a manipulated image, there is inconsistency in aberration in some of the parts of the image, which can be used to prove that the image is forged [9]. In other words, the aberration modeled for the parts of the image is seen with a discrepancy. The aberration seen in local parts of the host image is not consistent with the global aberration value for the complete image. Figure 5 shows the detection of such image forgery through red and green outline blocks that refer to inconsistent and consistent blocks respectively.

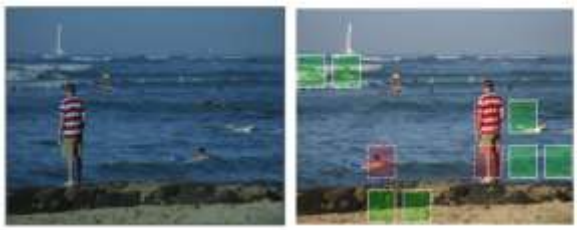


Fig. 5: The Red outline (dashed) blocks are inconsistent regions with respect to global aberration value. The green outline (solid) blocks denote consistent regions with respect to global value [9].

One of the drawbacks of this approach is that to find the global estimate of the complete image, the major part of the image must be authentic. On the contrary, if the major part of the image is forged, then, the global estimate of the image is itself inaccurate and can give false results. It also gives good results when the image is of good quality

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

because the chromatic aberration can be modeled better with images of high quality.

E. JPEG Ghosts: A way to detect passive forgery

JPEG ghost [10] is an effective way to detect forgery in a manipulated part of an image. The authors proposed a method in which the forgery in the parts of the image can be detected by compressing the image at different JPEG qualities followed by finding the difference between local minima in the image and that of the compressed image. This method is based on the idea that there exists a map in the local minima regions to the complete image. This difference indicates the regions that had undergone forgery in the image. The drawback of this technique is that this method is effective and gives accurate results only for those images in which the manipulated region is compressed with JPEG quality degradation as compared to the complete image.

F. Block-Grained Analysis for Image Forgery Localization of JPEG Images

In this method, the host image is first divided into 8x8 DCT blocks and each block is then checked for double compression [11]. This method is proposed to detect the region that has been compressed more than once. The accuracy of forgery detection is comparatively better as compared to the previous methods proposed for forgery detection for JPEG images. The idea behind this method is to compute the likelihood map that indicates the probability of compression in the DCT block. If the probability is greater than the threshold, it indicates that the image has been manipulated. Figure 6 shows the results obtained through the proposed method. The red region in the image indicates probability of double compression, whereas, the blue region in the image indicates its low probability [11].

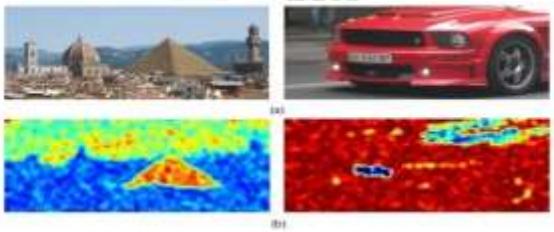


Fig. 6: Set of images in (a) contain two images having double JPEG compressions, non-aligned and aligned, respectively. Set of images in (b) shows the probability maps of the image corresponding to the respective images. Red/blue areas in the image show the probability as high/low of double compression [11].

G. Feature Based Clustering in JPEG Images

In this method, the idea under consideration is to differentiate between the regions in an image which is doubly compressed from that of singly compressed regions [12]. If any of the doubly compressed regions is present in an image, it gives a clue that the region has been manipulated. The method uses feature based clustering after converting the image into gray-scale image. The histogram of each block is computed and the kurtosis value for the number of pixels in each histogram is found. Finally, the clustering using k-means identify the blocks that were manipulated. The drawback of the method is that the false positives are produced when the host image contains a few feature values of the histograms, which are of doubly compressed regions matches with the histograms of the singly compressed region. On similar grounds, some of the doubly compressed regions can be identified as singly compressed.

H. Vector-Value Based Forgery Detection [13]

This method is an efficient way of determining Image Forgery as it compares the matrices or partitions of the host image, unlike the prevailing methods which worked by comparing pixels. The image is first subjected to Discrete Fourier Transform to get the non-overlapping blocks. The method eliminates the points which are found isolated by grouping the cells following a specific pattern. The process is applied iteratively until the resultant matrix was no more partitioned. The result of the method was the identification of the manipulated region in a forged image.

I. Deep Learning Approach for Forgery Detection

The method described in this approach is based on Deep Learning technique, which uses Convolutional Neural Network (CNN) capable of learning the hierarchical representations from the input RGB images automatically [14]. The CNN is first trained for identification of tampered images on a set of training images. The features of the patch are then used to train the SVM. The weights of the first layer of the CNN are initialized by the basic filter used in the calculation of Spatial Rich Model (SRM). The pre-trained CNN and SVM are then used to test the input image. The authors have used the CNN model that is based on the labelled patch samples based on forged boundaries. Figure 7 shows the architecture of the CNN used by the authors for this approach. After each layer, the feature map is reduced in order to identify the feature that can be used by the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

SVM classifier to give results. The drawback of this approach is that when the basic filters used while training the CNN are identical, the results are undesirable.

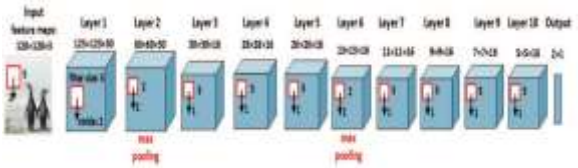


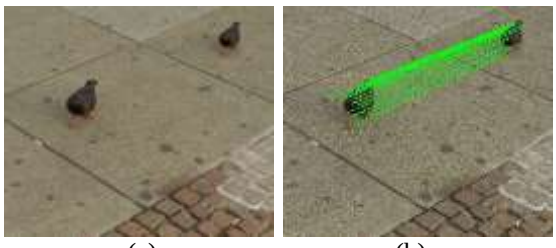
Fig. 7: Architecture of Convolutional Neural Network having 10-layers [14]

J. Image Forgery Detection using Zernike Moments

This method [15] uses the calculation of Zernike Moments of each block of the image under consideration. The vectors obtained are arranged in lexicographical order and the distance between the vectors is calculated. The threshold is applied to the distance and the suspicious blocks are listed. The method is rotation invariant and produces the same vectors even if the object is rotated. However, the method does not give good results when the forged object is small. Also, the false positives are produced due to the quantization of data and interpolation.

K. Copy-Move Forgery Detection using Auto Color Correlogram

This method [16] identifies the Copy-Move Image forgery, as, for a pair of arbitrary colors, Ci and Cj, it calculates the spatial correlation with the change in distance between them. The method uses 8z affine transform to make it rotation invariant. The Manhattan distance similarity calculated the distance between the color correlogram of each block and the values lesser than the threshold were concluded as the suspicious blocks. However, the 8z affine transformation made it highly extensive to space and ultimately to the computation. Figure 8 (a) shows the forged image with two identical birds. On input of the forged image, the implementation results are shown in Figure 8 (b).



(a) (b)

Fig. 8: (a) The Original Image, (b) the Forged image and (c) the results after implementation of approach [16]

III. COMPARATIVE ANALYSIS

Passive Forgery Detection techniques for digital images can be categorized on the basis of the type of forgery the technique is able to detect. The ways in which the techniques can be categorized are as follows:

1. Based on tampering operation
- Cloning or copy move
- Re-sampling
- Splicing

2. Categorization on the basis of Intrinsic Inconsistencies/Irregularities
- Existence of Optical Irregularities: Chromatic aberration, Inconsistencies in lighting, etc.
- Existence of Sensor irregularities: Noise in Sensor pattern (SNR), Camera response function, etc.
- Statistical irregularities: Statistics of Natural image, color features like Auto Color Correlogram, Zernike moments, etc.

The comparative analysis of Image Forgery Detection Approaches on the basis of their strengths, weakness and type of forgery is shown in Table 1.

Table 1: Comparative Analysis of Passive Image Forgery Detection Techniques

Approach	Type of Forgery	Strength	Weakness
Detection through Traces of Resampling	Image Composites	Shows high accuracy for images in which operations like rotation, resizing, etc.	Applicable only to images with regions having minimum compression in the image
Detection through Inconsistencies in Lighting	Image Composites	Shows high level of accuracy when the composite image contains parts of images having different sources of light and different light directions.	The approach is not applicable for the images where the lighting environment is complex.
Detection through	Copy-move	More effective for images in	Works weaker when the forged

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Chromatic Aberration		which the forged region is comparatively smaller than the complete image.	region is in greater ratio as compared to the complete image.
Properties of JPEG Compression	Copy-move	Accurate results when JPEG image has double compression in the image.	Low quality images can lead to show false results.
JPEG Ghosts	Copy-move, Image Composites	Detects forgery accurately when the regional discrepancy has undergone compression on lesser quality as compared to the parent image.	As the difference in quality of the forged and authentic regions decreases, the results become undesirable.
Analysis of Blocks Grained JPEG using Artifacts	Copy-move, Image Composites	Both the kinds of double compression, namely, aligned and non-aligned, which ultimately leads to forgery in JPEG images, can be detected through this approach.	Computationally intensive
Feature based clustering in JPEG Images	Copy-move, Image Composites	The doubly compressed images are distinguished from singly compressed images by k-means clustering applied to the kurtosis value of the number of pixels in the histogram.	False positives are produced as it is based on kurtosis value of number of pixels in the histogram.
Vector-value based forgery detection	Image	The comparison is done on vectors and not on pixels.	Highly computationally expensive
Deep Learning Approach for	Image	A CNN is trained on the training set of images. The weights of the first layer of the CNN are initialized by the basic filter used in calculation of Spatial Rich Model (SRM). The supervised SVM is also trained as per the prior information. The images are then tested for forgery.	If the basic filters used while training the CNN are identical, the results are undesirable.
Zernike Moments	Copy-Rotate-Move	By using the amplitude of Zernike Moments, the shape of the object is identified. The amplitude of Zernike Moments remains unchanged even if the object is rotated.	It does not give good results when the object in the image is of size smaller than the threshold. Also, false positives are produced due to quantization and interpolation
Auto Color Correlogram	Copy-Move	For a pair of arbitrary colors, C_i and C_j, it calculates the spatial correlation with change in distance between them. Rotation invariancy is achieved by using 8z affine transforms.	If the angle of rotation of the forged region is not a multiple of 45 degrees, false negatives are produced.

IV. CONCLUSION

Through the above analysis, we can see that many researchers have provided their efforts to categorize images as forged and authentic. The researchers have used various features to identify the forged regions in the input image. Out of the various approaches of image forgery, one of the most widely used is copy-move forgery (cloning), in which some part(s) of an image is copied and moved to same or another image in order to change the perspective of the user. Many algorithms are available for the identification of forged region(s) in a forged image. However, there are drawback(s) of using each one of them independently. The need of the hour is

to combine the available algorithms that reduce the drawbacks and provide more accurate judgment in a single pass.

V. REFERENCES

[1] H. Farid, "Digital doctoring: how to tell the real from the fake," Significance, vol. 3, no. 4, pp. 162–166, 2006.

[2] H. Farid, "Image forgery detection," IEEE Signal processing magazine, vol. 26, no. 2, pp. 16–25, 2009.

[3] P. K. Atrey, W.-Q. Yan, and M. S. Kankanhalli, "A scalable signature scheme for video authentication," Multimedia Tools and Applications, vol. 34, no. 1, pp. 107–135, 2007.

[4] Y.-F. Hsu and S.-F. Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency," in Multimedia and Expo, 2006 IEEE International Conference on, pp. 549–552, IEEE, 2006.

[5] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "Comofod - new database for copy-move forgery detection," in ELMAR, 2013 55th international symposium, pp. 49–54, IEEE, 2013.

[6] A. C. Popescu and H. Farid, "Statistical Tools for Digital Forensics," 6th International Workshop on Information Hiding, Toronto, pp. 128-147, 2004.

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on signal processing, vol. 53, no. 2, pp. 758–767, 2005.

[8] M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proceedings of the 7th workshop on Multimedia and security, pp. 1–10, ACM, 2005

[9] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proceedings of the 8th workshop on Multimedia and security, pp. 48–55, ACM, 2006

[10] H. Farid, "Exposing digital forgeries from jpeg ghosts," IEEE transactions on information forensics and security, vol. 4, no. 1, pp. 154–160, 2009

[11] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of jpeg artifacts," IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1003–1017, 2012

[12] G. Bhartiya, and A. S. Jalal, "Image forgery detection using feature based clustering in JPEG images," In Industrial and Information Systems (ICIIS), 2014 9th International Conference, pp. 1-5, IEEE, 2014

[13] M. Ranjani, and R. Poovendran, "Image Duplication Copy Move Forgery Detection Using Discrete Cosine Transforms Method," International Journal of Applied Engineering Research, Vol 11 no. 4, pp. 2671-2674, 2016

[14] Y. Rao, and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images." In Information Forensics and Security (WIFS), 2016 IEEE International Workshop on, pp. 1-6. IEEE, 2016

[15] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Information hiding, vol. 6387, pp. 51–65, Springer, 2010

[16] A. V. Malviya and S. A. Ladhake, "Pixel based image forensic technique for copy-move forgery detection using auto color correlogram," Procedia Computer Science, vol. 79, pp. 383–390, 2016

[17] M.-K. Hu, "Visual pattern recognition by moment invariants," IRE transactions on information theory, vol. 8, no. 2, pp. 179–187, 1962.