Industrial Science
Vol.1,Issue.4/April. 2014 ISSN : 2347-5420

AN ASSESSMENT OF DIGITAL IMAGE FORGERY DETECTION TECHNIQUES

Dhara Anandpara

Computer Engineering Department Parul Institute of Engg. and Technology Vadodara, India.

Abstract

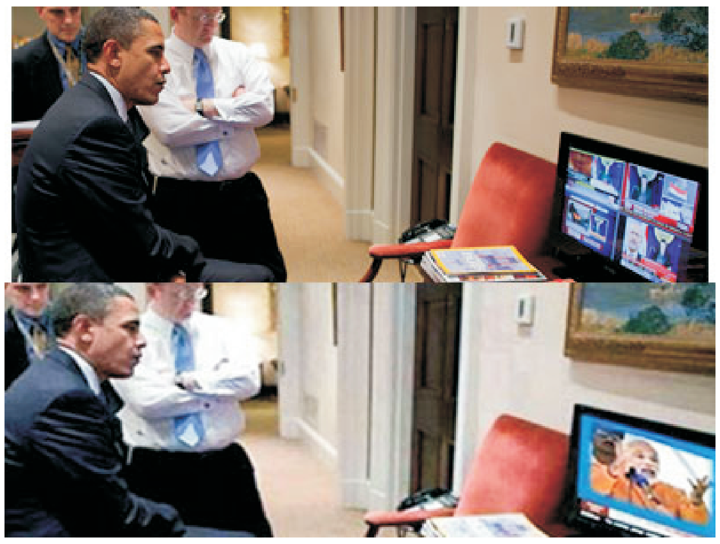
With advent of many tools in the digital images, image forgery is the big concern today in Digital Forensics Industry. Digital Image forgery is one of the well-known field in which one can change image in different ways using several powerful editing software's, as a result it become a serious social problem. For this, researchers continuously exploring new approaches to detect image forgery areas and change it to original pixel values if possible. In recent years, the detection of forged region has become one of the most active research topics in blind image forensics. Many techniques and algorithms have been proposed to process on post-processed images. This paper surveys these different techniques and its limitations and based on the outcomes it draws the line to exhibit the future concern areas in digital image forgery detection.

KEYWORDS:

Digital Forensics; image forgery detection; manipulation detection; copy-paste forgery detection

I.INTRODUCTION

In today's era Digital visual media represent one of the principal means for communication. As a consequence, today images and videos represent a common source of evidence. With undoubted benefits, accessibility of the digital media brings its own major drawbacks. Image processing experts can easily access and modify the contents and therefore its meaning, leaving visually detectable traces. Due to the availability of higher solution digital cameras, hi-tech personal computers, powerful software and hardware tools in the image editing and manipulating field, it become possible for someone to create, alter and modify the contents of a digital image and to violate its validation. From the past few years, manipulation of digital image has proliferated and can be found in courtrooms, fashion industry, scientific journals, tabloid magazine and internet etc. As a consequence, the modification of images for malicious purposes is now more common than ever. For e.g. in Figure 1, image which is now-a-days passing in social media as Barack Obama, an American President very interestingly watching Narendra Modi on TV, which is totally forged and altered with actual picture which was taken before 3 years in which Obama is seen watching a televised speech by the then Egyptian President Hosni Mubarak in the Outer Oval office. Digital Image Forensics is that branch of multimedia security that, together with Digital Watermarking, aims at contrasting and exposing malicious image manipulation [1].



Narendra Modi's speech on TV. Which is forged by original Upper image.

Due to its consequences, several techniques has been proposed in order to detect whether image has been forged or not. Digital images offers many attributes to propose tamper detection algorithm based on the parameter of color or brightness of individual pixels as well as image resolution and format. As a result, it helps to detect the forged or tampered areas in digital image.

The main goal of this paper is to scrutinize existing Copy-Move Forgery Detection (CMFD) techniques. Section 1 is the draft of the introduction, Section 2 follows with the different approaches, Section 3 will undergo inspection of approaches in more details, Section 4 will conclude.

II. APPROACHES OF DIGITAL IMAGE FORGERY

Generally digital image forgery can be apply by dividing them in two categories: those which produce the forgery working on a single image, and those that access the content of more than one image (i.e. composites).

A.Forgeries in Single Image

Manipulation within single image involves either deletion of undesired objects or altering region within the image itself. The forgers need to here, however, fill the deletion portion of the image with the other portion of the image being placed at the deleted region. Or it can be placement of new object taken from image and place again in the image itself. Forgers can even transform the image for better hiding the image content such as rotation, scaling, pixel distortion etc.

Image forgery can also be produced through in-painting techniques [9], Inspired by real techniques for painting restoration, in-painting methods fill the holes left by object removal by exploiting the information preserved in the regions surrounding the gaps. In particular, in-painting is based on an iterative process of smooth information propagation from the image to the region to be filled. The gap is gradually filled from the periphery to the centre, resulting in a perceived continuity in the final image. However, the algorithm struggles with filling highly textured areas.

Forgeries can be performed on a single image also without recurring to object removal. Image semantics can be modified by applying simple image processing techniques, such as histogram manipulation or contrast enhancement. Additionally, brightness and colour adjustment.[1].

B. Forgeries using multiple image sources

The insertion in an image of material originally coming from another source is one of the most powerful tools to overturn the message contained in visual media. Modern techniques and editing software allow easy creations of image composites (e.g. through layers superposition) obtaining results that are hardly detectable by the human eye (Figure 2). Blending and matting techniques are again applicable to mask the boundaries of the spliced regions and to give the image a more uniform aspect [1]. Also, the creation of image composites might require geometric transformation. Rotation, scaling and translation are often needed to make sure that the spliced object respects the original image perspective and scale. Geometric transforms typically involve re-sampling, which in turn calls for interpolation (e.g. nearest neighbor, bilinear, bicubic). The re-sampling process produces artifacts in the image histogram, and hence provides a useful cue for compositing detection.

It should be also taken into account that inserted material does not necessarily have to come from natural images. As computer graphics evolves, more and more realistic 3D objects can be modeled and rendered to be eventually spliced into an image composite. Furthermore, the extraction of 3D scene structure from images allows manipulating objects by morphing them: in this case, the splicing involves a remodeled (i.e. artificial) version of a part of the original image.

III. DIGITAL IMAGE FORGERY DETECTION TECHNIQUES

Digital forgery detection methods are categorized into active and passive (blind) methods. Active-based image forensic approaches include digital watermarks or signatures to authenticate the digital images. Digital watermark can be classified as robust, fragile and semi- fragile watermark. The watermark can be used in applications like copyright protection and ownership verification of digital media because they can resist multiple degradations (JPEG compression, geometrical distortions).On the other hand, the fragile watermark are used for content authentication and integrity attestation but robust to various modifications whereas semi fragile methods are robust to incidental modification such as JPEG compression, but fragile to other modifications [4]. But these methods require some pre-processing operations such as embedding watermark or signature-generation at the time of recording that may limit their application in practice[1].

In passive techniques digital image forensics operate in the absence of watermark or signature and leave no visible clues that indicate tampering i.e. they may alter the underlying statistics of a digital image [2].

The goal of blind image forensics is to determine the authenticity and origin of digital images without the support of an embedded security scheme (see e.g., [3]). Within this field, copy-move forgery detection (CMFD) is probably the most actively investigated subtopic. A copy-move forgery denotes an image where part of its content has been copied and pasted within the same image. Typical motivations are either to hide an element in the image, or to emphasize particular objects. A copy-move forgery is straightforward to create. Additionally, both the source and the target regions stem from the same image, thus properties like the colour temperature, illumination conditions and noise are expected to be well-matched between the tampered region and the image. The fact that both the source and the target regions are contained in the same image is directly exploited by many CMFD algorithms [1].

All copy-paste forgery detection techniques are used to detect duplicate regions in the digital images. A competitive copy-paste forgeries detection method should be able to cope with all scenarios, as it is not known beforehand how the forger applies the forgery.

The common and most straightforward way to search the copy-paste forgery is the comprehensive search that involves the image and its circularly shifted version are overlaid looking for closely matching blocks. This method is computationally expensive in performance and take (M X N)*2 steps for an image of size MxN .This approach is simple and effective for small sized images but not applicable where the copied region undergone some modifications. Another method to detect the copy paste forgery is the auto correlation but it requires the forged area to be large enough to give a detectable peak. This method does not have large computational complexity but still impractical to detect forgery in certain conditions.

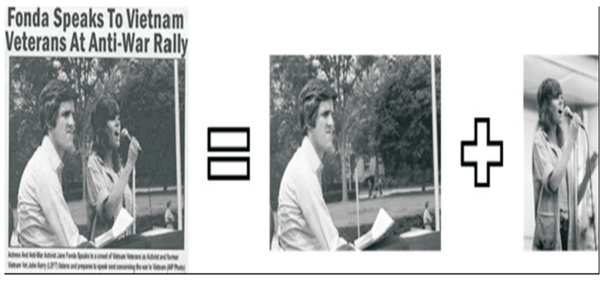


Fig 2: Mixed image from different images to outcome. Images are taken from [1].

In order to overcome these defects, we can broadly divide the copy- paste forgery detection into two categories such as block based techniques and keypoint based techniques.

A.Block- based Techniques

In these techniques, the original image is divided into the overlapping blocks and applying the transformations over the block to generate the feature vectors. Fridrich et al. [3] describes an efficient and reliable method by extracted DCT (Discrete Cosine Transform) coefficient and lexicographically sorting is performed over the extracted blocks which will detect the forged part although the copied area is enhanced, retouched or tampered image is saved in a lossy JPEG format. But they assume that copied region has not undergone any post-processing operation which is not always the case.

Later, Popescu et al. [4] proposed a technique based on the Principal component analysis (PCA) to reduce the dimensionality. These techniques are healthy to minor variations in the image due to slight noise addition and lossy compression but does not address the geometrical transformations. Experimental results demonstrate the robustness of this method to compression up to JPEG quality level 50.

On the other hand, G. Li et al. [5] proposes a method which reduces the time complexity. The given image is segmented into four sub-bands by applying (DWT) discrete wavelet transform, Singular Value Decomposition is performed on the low-frequency coefficients of the fixed-size blocks to reduce the dimension representation, and then lexicographically sorting is applied to SV vectors as a result duplicated image blocks are to be detected. Author showed its robustness to compression up to JPEG quality level 70.

Later on, B.Mahdian [6] defines the block representation calculated using blur invariants and aims to seek features that are invariant to the presence of blur artifacts that a falsifier can apply to make detection of forgery more difficult. H. Lin [7] describes a new efficient method based on PCA in which extracted featured vectors are sorted using the radix sort, in order to improve the time complexity. In their paper, this method is not applicable to detect the small copied regions as well as duplicated regions with rotation in some angles.

S. Ryu et al. [8] uses the Zernike moments that are invariant against possible rotation, the intentional distortions such as JPEG compression, blurring and additive white Gaussian noise but it does not show its strength against affine transformation and scaling. The magnitude of Zernike moments is calculated by extracting the feature vectors of a given blocks and lexicographically sorting is performed on each feature vectors and Euclidean distance is calculated to detect the forged image block.

Y. Huang [9] gives the improved performance on DCT- based method in which DCT coefficients are applied to each overlapping block to represent its features and Truncating is employed to reduce the feature dimensionality. In his paper, this improved method shows its robustness to detect the duplicated regions that are distorted by blurring, JPEG compression or additive white Gaussian noise.

S. Khan [14] proposed Discrete Wavelet Transform (DWT) to the input image by subdividing the image into overlapping blocks and then the duplicate blocks are detected by phase correlation as the similarity criteria. Author tries to reduce the time as compare to approach expressed in [9] to detect the forgery and also increases the accuracy of detection mechanism. Bravo [10] proposed a new method to detect the duplicate regions although it undergone to reflection, rotation and scaling. They use the colour dependent feature vector to reduce the number of comparisons in searching.

In general, first image is divided into overlapping blocks, and then feature is extracted and computed to find the duplicate blocks.

B.Key-point based Techniques

In Block based methods, often result in significant false positives, and is invariance to other transformations like flipping, brightness changes and blurring is hard to establish [11]. Recently, Keypoint based methods has been incited as digital image forgeries become common with the large number of transformations. Keypoint based methods relies on the identification and selection of high entropy image regions instead of blocks.

H. Huang et al. [19] describes an effective way to handle various transformations by extracting SIFT descriptors of an image that are invariant to scaling, rotation and changes in illumination etc. In his paper, this way has no estimation of the parameters of the applied geometric transformation to be performed and numerical results are also not evaluated and computed which shows the actual performance of methodology.

On the other hand, X. Pan et al. [20] again uses the SIFT features to detect duplicate image regions with high entropy without any image subdivision. It seeks the duplicated, erroneous and irregular region that are distorted with rotation, scaling, free-from affine transform, perspective projection, reflection or illumination adjustment by using features but SIFT algorithm fails to find reliable keypoints in regions with little visual structures because smaller regions have few key points and hard to detect. Later on, I. Amerini et al.[11] proposes SIFT features to shows its strength to detect a copy–move attack as well as to recover the geometric transformation over the cloned and replicated regions and also deal with multiple cloning. This method works by robust feature matching procedure and then perform clustering on the key-point coordinates to separate the cloned regions but SIFT features does not address flipping and illumination change of the cloned regions.

B.L.Shivakumar et al. [12] proposes a fast and robust method based on Speeded Up Robust Features (SURF) that detects duplication region of different size by using KD-tree algorithm for key-point matching which is more reliable. It also tries to minimize the false match for images, which having high resolution and shows its robustness to additive noise, geometric and photometric deformations whereas the small copied regions are not detected by this method.

In keypoint based methods, high entropy regions are investigated to detect the tampered region or forged areas.

Comparison of both block based techniques and key-point based techniques are given in table 1.

Block Based Techniques						
Year	**Method**	**Feature-Length**	**Block number (Block size)**	**Image size**	**Advantages**	**Shortcomings**
2003	DCT[4]	64	255,025 (8*8)	512x512	DCT is that the signal energy would be concentrated on the first few coefficients, while most other coefficients are negligibly small	Computational complexity is very high
2004	PCA[4]	32	255,025 (8*8)	512x512	Additive noise, Lossy JPEG compression and reduces the dimensionality	Low detection rate for small sized block and low SNR
2007	KPCA[6]	72	286,281 (20*20)	640x480	Support blurring, additive noise and contrast changes	Computational time increases due to similarity threshold
2009	FMT[15]	45	289(32*32)	200x200	Low computational time due to counting bloom filter	Does not robust to detect the rotation with arbitrary angles and scaling with large factor
2010	Zernike moments[8]	12	111969 (24*24)	400x320	adequate support for rotation	Does not address scaling
2010	DWT[5]	64	3249 (8x8)	64x64	Detection time decreases with adding noise increases	Duplicate regions with rotation through angles and scaled regions are not detected
2011	Bravo proposed method[10]	4	24*24	300x400	Less false alarms in images with little textural information	Does not support illumination change and blurring.
Key-Point Based Techniques						
2010	SIFT [10,11]	128	----	800x600	Support rotation, scaling and illumination changes	Illumination change and blurring parameters are not evaluated and does not support flipping and multiple cloning
2011	SURF[12,16]	64	----	3000 x 2400	Reduces the false match rate and fast as compared to SIFT	Small copied regions are not detected

CONCLUSION

As the copy-paste forgeries become common place, the need of forgery detection techniques is increasing to address various aspects of digital image forensics problem. Although there are many promising and innovative techniques but none of them give definite solution to a particular problem.

According to survey of multiple techniques in the field of copy- paste digital image forgery detection one can conclude that key point based methods are more robust to detect the duplicate regions that are subjected to geometrical transformations due to its low computational complexity and address other complex image processing operations as compared to block based methods. Digital image forensic is still growing area and a lot of research is needed to address the various challenging issues.

A novel technique can be proposed to overcome the shortcomings of above survey that will address the geometrical transformations and other image processing operations that make the forgery more real with low computational complexity.

REFERENCES

1.J. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners", In Multimedia Tools Applicat.Jan. 2011.
2.H. Farid, "A survey of image forgery detection", In Signal Process. Mag., Mar. 2009.
3.J. Fridrich, B. Soukal and Lukas, "Detection of copy-move forgery in digital images", in Proc. Digital forensics Res. Workshop, 2003.
4.Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", In Dept. Comput. Sci., Dartmouth College, Tech. Rep., 2004.
5.G. 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 Proc. IEEE ICME, Beijing, China, 2007.
6.B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", In Forensic Sci. Int., vol. 171 no. 27–3, 2007.
7.H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection", In WSEAS Trans. Signal Process., vol. 5, no. 5, 2009.
8.S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using zernike moments", in Proc. Int. Workshop Information Hiding, Springer , pp. 51–65, 2010.
9.Y. Huang,W. Lu,W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery" in images, Forensic Sci. Int., vol. 206, no. 1–3, 2011.
10.S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling", in Proc. Int. Conf. Acoustics, Speech and Signal Processing, 2011.
11.I . Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery",IEEE Trans. Inform. Forensics Security, vol. 6, no. 3, Sept. 2011.
12.B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo , "Detection of Region Duplication Forgery" in Digital Images Using SURF, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, 2011
13.H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm", in Proc. IEEE Pacific-Asia Workshop Computational Intelligence Industrial Applic., 2008.
14.S.Khan and A.Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform", International Journal of Computer Applications ,Vol. 6– No.7, September 2010.
15.S. Bayram, H. Sencar, and N.Memon, "An efficient and robust method for detecting copy-move forgery", in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Apr. 2009.
16.L. Jing and C. Shao, "Image Copy-Move Forgery Detecting Based on Local Invariant Feature, Journal of multimedia", vol.7, No.12012.