International Journal of Research in Engineering, Science and Management
Volume-3, Issue-2, February-2020
www.ijresm.com | ISSN (Online): 2581-5792

An Approach for Image Forgery Detection

Pooja Bhole[1], Dipak Wajgi[2]
[1]*M.Tech. Student, Department of Computer Science and Engineering, St. Vincent Palloti College of Engineering and Technology, Nagpur, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, St. Vincent Palloti College of Engineering and Technology, Nagpur, India*

***Abstract*: With the high resolution of the advanced image handling a computerized picture can be effectively controlled. An image is being generally accepted as a proof of occurrence of the past events. The low-cost hardware and software tools make easy to create and manipulate digital images with no obvious traces. The digital image forgeries are increases in different application fields and made negative marking to accept the integrity and authenticity of the digital images. In this paper, various types of forgery image and detection techniques have been explained.**

***Keywords*: Copy-move, Digital image, Forgery detection, Image splicing.**

1. Introduction

Now a days, images have become very useful in broadcasting media. There is a belief that the image speaks more truth about the incident or the situation captured than the words. Professional knowledge was required to manipulate the images generated by traditional cameras with sophisticated dark-room equipment, which is difficult to do so for average users. The process of recording, sharing and storing of large number of images is possible by everyone. With the time of digital images most of the image processing techniques have been proposed.

Images are edited using the software tools which are subjected to several processing stages and the forgery in an image cannot be detected by the human vision. The modified images are appearing at an increasing rate leading to the decrease of trust in the visual content. With the advanced development of forgery tools, technology has been innovated to check the originality of the image information.

Forgery detection technique is one of the verification methods, which assumes that the original images has some native patterns, which are introduced by the various imaging devices. These patterns are always consistent in the original images and altered after some forgery operations. The image forgery detection has become difficult, because of the advanced and sophisticated processing tools. [17]

2. Literature Review

Digital image forgery detection techniques are broadly classified into two categories namely active and passive methods. Methods used in the active authentication includes digital signature [1] and digital watermarking [2]. Passive authentication includes pixel-based technique [3], format-based technique, physical environment-based technique and geometric based technique.

A. Active Authentication

Numbers of tools exists to create or manipulate the digital image, so one can't easily trust on any digital document which is provided as legal evidences. So, the authenticity of the image is to be checked. Image is said to be modified or manipulated if the operation like scaling, rotating, blurring, brightness adjusting, change in contrast, etc. or combination of these operations are performed on an image. In active authentication techniques previous information about the image is indispensable to the process of authentication. It is agitated with data hiding where some code is embedded into the image at the time of generation. Verifying this code authenticates the originality of image. Active authentication methods are classified into two types: digital signature and digital watermarking.

In [1], digital signature has been proposed for demonstrating the authenticity of digital document using a sort of mathematical scheme. A robust bit is extracted from the original image. An image is divided into 16*16 pixels blocks. On each random matrix a low pass filter is applied repeatedly to obtained N random smooth pattern.

In [2], Digital watermarking has been proposed for authentication of audio data, still images and visual multimedia. A visually undetectable watermarking schema is also available which can detect the change in single pixels and it can locate where the change occurs. One uses a checksum schema that it can add data into last most significant bit. Others add a maximum length linear shift register sequence to the pixel data and the watermarked image and then identify the watermark by computing the spatial cross-correlation function of the sequence.

B. Passive Authentication

Passive forgery detection technique uses the received image only for assessing its originality without any watermark or signature of the original image from the sender. It is based on the assumption that digital image forgeries may leave no visual clues of having been tampered with, they may highly disturb the underlying statistics property or image consistency of a

natural scene image which introduces new crop resulting in various forms of inconsistencies. This unpredictability can be used to detect the forgery. This technique is popular as it does not need any previous information about the image. Existing techniques identify various track down of tampering and detect them separately with localization of tampered region.

Pixel based technique: Pixel based forgery detection technique are classified into three categories: Copy-move, Image splicing and Image retouching.[3]

C. Copy-move

Copy-move is the common photo tampering and most popular technique because of the ease with which it can be carried out. It involves copying of some area in an image and moving the same to some other area in the image. Since the copied region belong to the same image therefore the dynamic range and colour remains compatible with the rest of the image [4]. Along with the copy move operation, image editing related operations such as rotation, colour, scaling, blurring, compression and noise addition are added to the original image. This is done in order to make the forged part unnoticed by the human vision. The detection of some parameters like noise, colour from the forged is not possible to differentiate.

In [5], Gopi et al., developed a model to detect image tampering that used auto regressive coefficients as feature vector and artificial neural network classifier. The digital forgery is identifying 77.67% of modified images were used to train ANN and 94.83% dataset forged images was used.

In [6], Popescu and Farid suggested a method using principal component analysis (PCA) for the overlapping square blocks. Accuracy of 100% for block size of 160x160 and 50% for block size of 32x32 was obtained. This method has reduced complexity and is highly discriminative for large block sizes

In [7], presented a method that detects duplication using two robust features based on DWT and kernel principal component analysis (KPCA). KPCA based projected vectors and multi resolution wavelet coefficients ensuring to image-blocks are arranged in the form of a matrix. This method removes the off-set frequency threshold and in other detection methods frequency were manually adjusted.

In [8], Kakar and Sudha developed a new technique-based on transform-invariant features which detecting copy-paste forgeries but requires some post processing based on the MPEG-7 image signature tools. Feature matching that uses the inherent constraints in match feature pairs so as to improve the detection of cloned regions is use which results in a feature matching accuracy of more than 90%.

D. Image Splicing

Image splicing is a method of combining two or more images to make it a composite (single) image. When images are spliced, resulting image shows lines, edges, regions and blur to merge in the image so that the human vision is not able to detect the forgery.

In [9] authors have implemented the forgery detection of spliced image based on, watermarking where two images are combined to create a spliced image and watermark is recovered from the image which shows the presence of some noise which proves that tampering has been done to the watermarked image.

In [10] author gives an example that makes use of the sharp boundaries in colour images. The technique looks for the consistency of colour division in the neighbourhood pixels of the boundary. The author suggests that the irregularity at the colour edge is significant evidence that the image has been tampered.

E. Image retouching:

Image retouching is one of the types of image forgery tool which is most commonly used for aesthetic and commercial applications. Retouching operation is carried out mostly to enhanced or reduce the image features. Retouching is also done to create a convincing composite of two images which may require rotation, stretching or resizing of one of the images.

In [11], a classifier is designed to measure distortion between the doctored and original image. The former may consist of many functions as change in brightness and blurring, Again the classifier performs well in case a number of operations are carried out on the image.

Two novel algorithms were developed in [12] to detect the contract enhancement involved manipulations in digital images It focuses on the detection of global contrast enhancement applied to JPEG- compressed images. Another algorithm is same paper proposes to identify the composite image created by enforcing contrast adjustment on either one or both source regions.

Format based technique: Image alteration does not prove malicious tampering, as in the cases of colour/contrast adjustment for image enhancement, and file format conversion for saving storage space. These modifications do not fundamentally change the contents of the original image, while malicious tampering will alter the meaning of the image, such as removing, adding and modifying an object in a scene. Malignant manipulations, in a collaboration with subsequent operations such JPEG compression, contrast adjustment, blurring, etc., would make forgeries hard to detect. Therefore image-alteration detection can determine whether the images are original and help with further analysis.

In [13], [14], authors have proposed a method to identify the bitmap compression history. In this method, given an image which is saved in bitmap format, to check whether it has been previously JPEG-compressed, and further to estimate which quantization matrix has been used. This method assumes that if there is no compression the pixel differences across blocks should be similar to those within blocks, while they should be different due to block artefacts if the image has been JPEG-compression.

Physical based technique: Technique is based on three dimensional interactions between physical object, light and the camera. Difference in lighting across an image can be utilized as proof of altering. This is work on the basis of the lighting

Table 1
Comparison of different techniques

Titles	Extracted Feature	Classifier	Detection Accuracy
"Detecting digital image splicing in the chroma spaces" [2]	Chroma Components from grey level co-occurrence matrix	SVM	90.5%
"Digital image forgery detection using artificial neural network (ANN) & auto regressive coefficients" [5]	Auto regressive coefficient	ANN	94.83%
"Exposing digital forgeries by detecting the duplicated image regions" [6]	PCA of overlapping block	Lexicographical sorting	50%- small block 100%-16x16 block
"Exploring the duplicated regions in natural images" [7]	DWT & KPCA	Point based duplication detection algorithm	95.55%(DWT) 90.94%(KCPA)
"Exposing the post processed copy-paste forgeries through transform- invariant features" [8]	transform-invariant	Image MPEG-7 Signature tools	90%
"Image splicing detection using colour edge inconsistency" [10]	Colour sharpness and difference of single value between different channels	LDA	90%
"Contrast enhancement-based forensics in the digital images" [12]	DCT of overlapping block	Lexicographical Sorting	96.1%

environment under which an article or picture is caught. Lighting is a key factor for capturing an image. These techniques are isolated into three classifications like light direction (2-D), light direction (3-D) and light environment. These techniques estimating the direction of an illuminating light source within one degree of freedom to detect forgery. By estimating direction of light source for different objects and people in an image, inconsistencies in lighting are uncovered in the image and tampering can be detected.[15]

In [16] Johnson and Farid estimated 3-D direction to a light source by means of the light's reflection in the human eye. These reflections called specular highlights are powerful clue as to the location and space of the light sources. Inconsistencies in location of the light source can be used to detect tampering.

In [17], author proposed a technique which infers that methods based on forgery detection using 2D lighting system can be fooled easily and gave a promising technique based on shape from shading. This procedure is more general but the issue of estimation of 3D shapes of objects remains.

Geometric based techniques: Geometric based technique basically based on principal point i.e. projection of the camera centre onto the image plane, that make measurement of the object in the world and their position relative to camera.

In [18], the authors have analysed the physical differences in generation between photographic images and CG, e.g., the sharp structures in CG images and gamma correction in photographic. The method extracts the geometry features based on the rigid body moments for source identification. The experimental results show the effect of the proposed method with a classification accuracy of 83.5%, which exceed the prior method.

3. Conclusion

In the last decennary many forgery detection techniques have been proposed. In this paper, a brief survey of Digital image forgery categories and its detection methods have been presented. An attempt is made to bring in various potential algorithms that denote improvement in image authentication techniques. From the knowledge of the image authentication techniques it is inferred that passive techniques which need no previous information of the image under consideration have a significant advantage of no requirement of special equipment's to embed the code into the image at the time of generation, when compared to active techniques.

As discussed earlier, the techniques which have been developed till now are capable of detecting the forgery and only a few can localize the tampered area. There are number of drawbacks with the presently available technologies. First, all systems require human clarification and thus cannot be automated. Second being the problem of localizing the forgery.

References

[1] Doke K K, Patil S M. Digital signature scheme for image. International Journal of Computer Applications. 2012
[2] Zhao X, Li J, Li S, Wang S. Detecting digital image splicing in chroma spaces. In international workshop on digital watermarking 2010.
[3] Bravo-Solorio S, Nandi A K, Automated detection and localization of duplicated regions affected by reflection, scaling and rotation in image forensics. Signal Processing 2011.
[4] Popescu AC, Farid H. Exposing Digital Forgeries in Color Filter Array Interpolated Images. IEEE Transactions on Signal Processing. 2005
[5] E. Gopi, N. Lakshmanan, T. Gokul, S. Ganesh and P. Shah, Digital image forgery detection using Artificial Neural Network (ANN) and Auto Regressive Coefficients, Proc. Canadian conference on electrical and computer engineering, 2006
[6] A. Popescu and H. Farid, exposing digital forgeries by detecting the duplicated image regions.
[7] M. Bashar, K. Noda, N. Ohnishi and K. Mori, "Exploring Duplicated regions in Natural images", IEEE Transaction Image Process, 2010.
[8] P. Kakar and n. Sudha, "Exposing postprocessed copy-paste forgeries through transform- invariant features", IEEE Trans Information Forensics Security. (2012)
[9] D. Vaishnavi and T, Subashini, Image tamper detection based on edge image and chaotic arnold map, Indian Journal of Science and Technology, 2015.
[10] Z. Fang, s. Wang and X. Zhang, Image splicing detection using color edge inconsistency, 2010 International Conference on Multimedia Information Networking and security, 2010.
[11] Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B. A classifier design for detecting image manipulations. In image processing international conference on 2004. IEEE.
[12] Cao G, Zhao Y, Ni R, Li X. Contrast enhancement-based gorensics in digital images. IEEE Transactions on Information Forensics and Security, 2014.
[13] Fan z, de Queiroz r. Maximum Likelihood Estimation of JPEG Quantizer table in the Identification of bitmap compression history. In international conference on image processing proceedings 2000. IEEE.

[14] Fan Z, De Queieoz R. Identification of bitmap compression history: Quantizer Estimation and JPEG Detection.
[15] Johnson MK, Farid H. Exposing digital forgeries by detection inconsistencies in lighting. In proceedings of the 7th workshop on multimedia and security 2005.
[16] Farid Hany and Johnson MK. Exposing Digital Forgeries Through Specular Highlights on Eye.
[17] Rajath B, Sunitha K, "Survey on Passive Image Tampering Detection" April 2016.
[18] Chang SF, Hsu J, Xie L, Tsui MP. Physics-Motivated Features for Distinguishing Computer Graphics and Photographic Images.
[19] Farid H. Image forgery detection. IEEE Signal Processing Magazine. 2009. Digital Watermarking", Norwood, MA: Artec House, 2000.
[20] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital watermarking Saan Fransisco", CA: Morgan Kaufmann, 2002.
[21] Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security, 2006.