IMAGE FORGERY DETECTION BY USING MULTIPLE APPROACHES

Dr. KHETAVATH SEETHARAM
Associate Professor, Department of ECE, CITS Warangal

ABSTRACT: As we are living in the today's digital world in which all type of advancement are becoming possible and at the same time the use of images have been increasing day by day in our lives, the motivation to make manipulation of images also increases simultaneously. This type of image forgery is going on increasing day-by-day. In this paper, we are performing a review of this Image forgery technique. There are two kinds of techniques for image forensics: one is active protection, and the other is passive detection. The main types of Image forgery techniques are Image Splicing, Copy-Move forgery used mainly for making tempered photographs are studied in more detail in this paper. As the forgery of Images is growing day-by-day, it is very much necessary to develop tools for detection as which image is true and which is forgery. We study on of the most powerful technique like the SVM classifier, Pixel-based and partition-based to detect forgery images.

I. INTRODUCTION

As the use of images have been increasing day by day in our lives, with the introduction of digital technology, The forgery of digital image has become more and more simple and indiscoverable. Today's digital technology had begun to erode the integrity of images and image counterfeiting and forgeries with the move to the world of Megapixels, opens a new door to the dark-side of it. We are living in an age, where anything can be manipulated or altered with the help of modern technology. With the increasing applications of digital imaging, different types of software tools are introduced for processing images and photographs. They are used to make forge images to make it look real or objects can be added or deleted. For decades, photographs have been used to document and they have used as evidence in courts. Although photographers are able to create composites of analog picture. But this process is very time consuming and requires expert knowledge so it is hard to implement than digital pictures. Today, however, powerful digital image editing software makes image modifications straightforward [1]. Today's digital technology has begun to remove trust in our knowledge, as from the magazines, to fashion world and in scientific journals, political campaigns, courts and the photo that come in our e-mail. In all of these forged photographs are appearing with a more frequencies and sophistication. In the increase in the availability of multimedia data in digital form has come to a tremendous growth of tools to manipulate digital multimedia contents.

The process of creating fake image has been tremendously simple with the introduction of new and powerful computer graphics editing software which are freely available as Photoshop, GIMP, and Corel Paint Shop. Today, this powerful image processing software's allow people to modify photos and images conveniently and un perceivably. Now days it creates a big challenge to authenticate images. Image forgery means manipulation of the digital image to conceal some meaningful or useful information from it. Sometimes it is difficult to identify the edited region from the original image. The detection of a forged image is driven by the need of authenticity and to maintain integrity of the image. The survey has been done on existing techniques for forged image and it highlights various copy–move detection and splicing detection methods based on their robustness and computational complexity [2].

A forgery detection method that exploits suitable inconsistencies in the color of the illumination of images. To achieve this, we incorporate information from physics- and statistical-based illuminate estimators on image regions. We try to extract texture- and edge-based features from the illuminate estimates. These features are provided to a machine-learning approach for making decision automatically. The classification performance using an SVM meta-fusion classifier is promising. A SVM classifier is trained for using statistical features of pattern noise for classifying smaller blocks of an image. SVM classifier is used which have similar functional form to neural networks. Image, texture and pixel value based features are extracted and analyzed from the images. Then has values are calculated for these features. The process consists of two phases, which are training phase, and a testing phase.

For each image in the database the hash value is generated by image hashing. These hash values can be used for content-based image retrieval, indexing image in database, and for authenticating, avoided and mitigate the forgery of digital images [3], etc. To ensure trustworthiness, multimedia authentication techniques have emerged to verify content integrity and prevent forgery. Experimental results show that even slightest of image tempering can be detection with the proposedtechnique can lead to provide authentication as the provided image is trusty.

In this paper, we are giving firstly the classification of the Image forgery approaches, which mainly consist of Active approach and Passive approach. In the third section, we are giving three types of image forgery techniques. In further section, we provide the possible image tempering detection techniques based on the SVM classifier. Finally, in the last section we conclude the paper.

II. CLASSIFICATION OF IMAGE FORGERY TECHNIQUES

There are two kinds of techniques for image forensics: one is active protection, and the other is passive detection. Which again consist of many different methods, as shown in below figure [5]:

A. Active Approach

In this active approach, the digital image requires some kind of pre-processing such as watermark embedded or signatures are generated at the time of creating the image. However, in practice this would limit their application. Digital watermarking [4] and signature are two main active protection techniques, as something are embedded into images when they are obtained. We can detect the Image is tampered, if special information cannot be extracted from that obtained image. Watermarking is such a method of active tampering detection, as a security structure is embedded into the image, but most present imaging devices do not contain any watermarking or signature module and that are similar to the application of active protection. This structure is used for integrity evaluation in the sense that if any discrepancy is found with the structure then the image is tampered and an inverse analysis over the structure is done to locate tampered Regions of the image. In recent times, various schemes are proposed for providing security to the image, which is analogous to the concept of watermarking like, message authentication code, image hash, image checksum and image shielding as a counterpart to it.

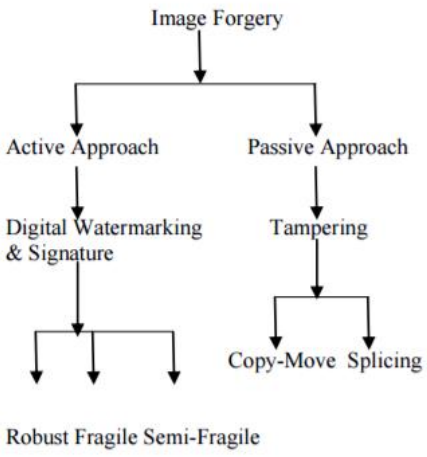

Fig. 1. Classification of Image forgery approaches

B. Passive Approach

Passive image forensics is usually a great challenge in image processing techniques. There is not a particular method that can treat all these cases, but many methods each can detect a special forgery in its own way. The stream of passive tampering detection deals with analyzing the raw image based on various statistics and semantics of image content to localize tampering of image. Neither construct is embedded in the image and nor associated with it for security, as like active approaches and hence this method is also known as raw image analysis. The localization of tampering is solely based on image feature statistics. Hence, algorithms and methods of detection and localization of image based on passive tampering vary depending upon the type of security construct used. Nevertheless, passive tampering detection typically aims for localization of tampering on raw image.

III. TYPES OF IMAGE FORGERY

A. Image Retouching:

Image Retouching is considered as less harmful kind of digital image forgery than other types present. In case of image retouching original image does not significantly changes, but there is enhancement or reduces certain feature of original image. This technique is popular among magazine photo editors. This type of Image forgery is present in almost all-magazine cover that would employ this technique to enhance certain features of an image so that it is more attractive. Actually, the fact is that such enhancement is ethically wrong.

B. Image splicing or photomontage:

This technique for making forgery images is more aggressive than image retouching. Image splicing is fundamentally simple process and can be done as crops and pastes regions from the same or separate sources. This method refers to a paste-up produced by sticking together images using digital tools available such as Photoshop. In Image Splicing technique there is composition of two or more images, which are combined to create a fake image. Examples include several infamous news reporting cases involving the use of faked images. Fig. 2 below shows how to create forge Image; by copying a spliced portion from the source image into a target image, it is a composite picture of scenery which is forge image.

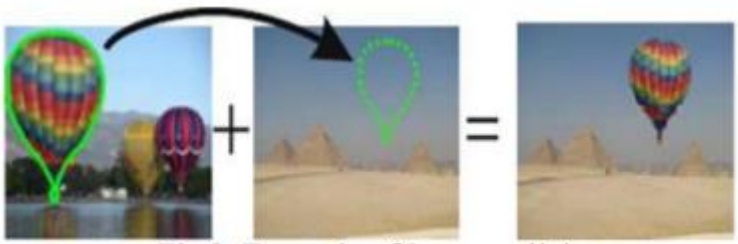

Fig.2. Example of Image splicing

C. Copy-Move Attack:

The copy move forgery is popular as one of the difficult and most commonly used kind of image tampering technique. In this technique, one needs to cover a part of the image in order to add or remove information. In the Copy-Move image, manipulation technique a part of the same image is copied and pasted into another part of that image itself. In a copy-move attack, the intention is to hide something in the original image with some other part of the same image [8]. The example of Copy-Move type is as shown in below figure 3 below. The original image contains only three missiles and its Copy-Moved version on the right has four missiles. Fig.3. Example of Copy-Move Attack on Images

Fig.3. Example of Copy-Move Attack on Images

IV. IMAGE FORGERY DETECTION AND PREVENTION TECHNIQUES

A. SVM Classifier:

SVM classifier is employed for forgery detection, as accuracy of detecting forgery is enhanced by using SVM classifier. Detection of forge Image is done using SVM classifier on systematic basis by designing a simple process consisting of two phases, which are training phase and testing phase [9]. In the training phase, a database is created and trained with a number of images.

RSA key is also set in training phase and the user is asked to enter the same key in testing phase for detecting the user is an authorized person. Some Pre-processing is done on the images by converting into gray scale from RGB. Then feature extraction is done by analyzing images, their Pixel values and texture analysis. After that, Hash values are calculated for the above extracted features.

The text and image classification, handwriting recognition, and bioinformatics are all complex operation and bio sequence analysis, which are largely based on Images, are handle by SVM classifier. Actual working of SVM Classifier determines the decision boundaries in the training step and their methods can provide good generalization in high dimensional input spaces. The concept of decision planes defining decision boundaries.

Which is one that separates between a set of objects having different class memberships, this concept is important as SVM classification is based on this. Classification with SVM supports both binary and multiclass targets, which finds the vectors i.e. "support vectors" that define the separators giving the widest separation of classes [10].

Neural networks and radial basis functions, which are popular data mining techniques performing same function as SVM. However, neither of these algorithms has the well founded theoretical approach to regularization, which creates the need of SVM. The SVMs map the original data points from the input space to a high dimensional, or even infinite-dimensional, making classification problem simpler in feature space. This mapping is done by making a suitable choice of a kernel function.

B. Copy- Move Forgery Detection Using Pixel-Based Approach

This Algorithm is based on Pixel Based approach. Its actual working is done as; firstly, dyadic wavelet transform (DWT) is applied to the input image. This transform yield the original Image in a reduced dimension representation, i.e., LL1 sub-band. Then this LL1 sub-band are divided into sub-images [11]. To compute the spatial offset (Δx, Δy) between the Copy Move regions the phase correlation is adopted. The Copy-Move regions can easily located by pixel matching, that shifts the input image according to the offset and calculate the difference between its shifted version and the original image. In the final step, the Mathematical Morphological Operations (MMO) are used to remove isolated points to improve the location.

C. The partition-based copy-move forgery detection approaches:

Most of the partition-based copy-move forgery detection approaches are classified as block-based approaches and Non- block-based approaches, both are briefly describe as follows:

1. Block-Based Approaches:

Firstly, some Pre processing as like the color conversion is done on the taken Images. In fact, many existing detection methods require a merger of the red, green, and blue colors as they operate on gray scale images [12].

The fact is that in a copy-move technique to make forgery, the source and the target regions are both located in the same image hence, the forged image must exhibit at least two similar regions. It helps to avoid the high computational cost of the exhaustive search by dividing into blocks and the comparison is done at a block level. The blocks can be either square or circular.

In the third step, features are extracted using any of the transformation like Discrete Cosine Transform (DCT), Wavelet-Based, etc. After the extracting the features, copy-move pairs are identified by matching those features, which can be done easily by searching the blocks with similar feature vectors.

The single similarity criterion is not enough to decide on the presence/absence of duplicated area in the corresponding image so, for those different algorithms are used like the same affine transformation selection (SATS) in [13], the multi hop jump (MHJ) algorithm, etc. The duplicated regions map obtained from the previous step needs to be further processed, which can be done sometimes by morphological post processing.

2. Non block-Based Approaches:

2.1. Segment-Based Approaches:

One approach to identifying copy-move forgeries involves partitioning the image into segments so that, the segment is relatively homogeneous and a single segment fully contains an object. For the input image taken as „I", the noise image considering as computed and for each segment of I. Then corresponding noise segment Sn is extracted from In. Finally, histograms of the extracted noise segments Snare compared for similarity check [14], which leads to the detection of the forgery image.

2.2. Sub image-Based Approaches:

To detect copy move forgeries, other methods that partition the image into sub-images of same size. The low-frequency sub band of the wavelet decomposition of the input image [15] is first divided into four non-overlapping sub images. To evaluate the spatial offset between the copied region and the pasted one, the phase correlation between every pair of sub-images is calculated. Then, the location of the forgery is get by shifting the input image in-line with the obtained offset and subtracting this shifted image from the original input image.

V. CONCLUSION

In this paper, we studied that, due to the advancement in the digital software's manipulation of digital images has become easy. As powerful computers, advanced photo-editing software packages and high resolution capturing devices are invented. Out of all the cases of digital image forgery, they can be categorized into two major groups as active and passive approaches, based on the process involved in creating the fake image. We studied the types of image forgery as, Image Retouching, Image Splicing, and Copy-Move Attack. As it is the vital need to make trust in all images and photographs we further studied the techniques for detection of any kind of Image forgery, which are based on different approaches. To ensure trustworthiness, multimedia authentication techniques have emerged to verify content integrity and prevent forgery of images.

REFERENCES

[1] de Carvalho, T.J.Riess, C. ; Angelopoulou, E. ; Pedrini, H., "Exposing Digital Image Forgeries by Illumination Color Classification" Information Forensics and Security, IEEE Transactions on ,June 2013.

[2] A.C. Popescu, and H. Farid, "Statistical Tools for Digital Forensics", in Proc. the 6th International Workshop on Information Hiding, Toronto, Canada, 2004.

[3] Kekre, H.B. ; MPSTME, NMIMS Univ., Mumbai, India ; Mishra, D. ; Halarnkar, P.N. ; Shende, P. , "Digital image forgery detection using Image hashing",Advances in Technology and Engineering (ICATE), 2013.

[4] W.N. Lie, G.S. Lin, and S.L.Cheng, "Dual Protection of JPEG Images Based on Informed Embedding and TwoStage Watermark Extraction Techniques", IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 330- 341, Sep. 2006.

[5] Advance in Image Forgery Techniques [Online] available:http://link.springer.com/chapter/10.1007%2F9 78-3-642-30157-5_71.

[6] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205-214, June 2006.

[7] W.H. Li, and B. Wang, "A Statistical Analysis on Differential Signals for Noise Level Estimation", in Proc. the 6th International Conference on Machine Learning and Cybernetics, Hong Kong, China, Aug. 2007, pp. 2150- 2153.

[8] Ashima Gupta, NisheethSaxena, S.KVasistha, "Detecting copy move forgery using DCT",International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153 .

[9] V.P.KAVITHA, M.PRIYATHA, "A Novel Digital Image Forgery Detection Method Using SVM Classifier" IJAREEIE, Vol. 3, Issue 2, February 2014.

[10] Anita Sahani, K.Srilatha, "Image Forgery Detection Using Svm Classifier", International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering, Vol. 3, Issue 3, March 2014.

[11] PradyumnaDeshpande,PrashastiKanikar, "Pixel Based Digital Image Forgery Detection Techniques", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 3, May-Jun 2012.

[12] Xu B, Liu G, Dai Y. A fast image copy-move forgery detection method using phase correlation. 4th International Conference on Multimedia and Security (MINES '12); November 2012; Los Alamitos, CA, USA. IEEE Computer Society; pp. 319–322.

[13] Zimba M, Xingming S. Detection of imageduplicated regions affected by rotation, scaling and translation using block characteristics of DWT coefficients. International Journal of Digital Content Technology and Its Applications. 2011; 5(11):143–150.

[14] Muhammad N, Hussain M, Muhamad G, Bebis G. Advances in Visual Computing. Vol. 6939. Berlin, Germany: Springer; 2011. A non-intrusive method for copy-move forgery detection; pp. 516–525.