A Review of Image Forgery Detection Technique Using Different Transform Function

Ashish Kumar Sharma, Amit Mishra, Shiv Kumar Sahu

Abstract: Image forgery detection is very important tool in digital forensic. The forgery detection tool detect the forged image area or forged image in terms of fake image and duplicate image. For the detection of image forgery various methods are used such as pixel based operation and transform based operation. The pixel based operation used the matching and segmentation technique and the transform based technique used feature based image forgery detection. In this paper present the review of image forgery detection technique using different transform function. The transform based function is very efficient for the processing of image forgery detection.

Keywords: - Image Forgery, Transform Function, Block Matching, Segmentation

I. INTRODUCTION

Image forgery detection is important area of digital image forencis. The rapid growth of image processing software's and the advancement in digital cameras has given rise to large amounts of doctored images with no obvious traces, generating a great demand for automatic forgery detection algorithms in order to determine the trust worthiness of a candidate image[1]. A forgery detection algorithm should be passive, requiring no prior information about the image content or any protecting methods like watermarks. According to the Wall Street Journal, 10% of all color photographs published in United States was actually digitally altered and retouched. The scientific community has also been subject to forgeries. The authenticity of photographs has an essential role as these photos are popularly used as supporting evidences and historical records in growing number and wide range of applications from forensic investigation, journalistic photography, criminal investigation, law enforcement, insurance claims and medical imaging. Image forgery has a long history [8, 9]. The digital watermarks also offer forgery detection. Few techniques use a checksum on the image data which is embedded in the least significant bits of certain pixels. Others add a maximal length linear shift register sequence to the pixel data and identify the watermark by computing the spatial cross correlation function of the sequence and the watermarked image. Watermarks can be image dependent, using independent visual channels [3], or be generated by modulating JPEG coefficients. These watermarks are designed to be invisible, or to blend in with natural camera or scanner noise. Visible watermarks also exist;

Revised Version Manuscript Received on May 23, 2016.

Ashish Kumar Sharma, M-Tech Scholar, Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P.). India.

Amit Mishra, Assistant Professor & Coordinator, Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P.). India.

Dr. Shiv Kumar Sahu, Associate Professor & Head, Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P.). India.

IBM has developed a proprietary visible watermark to protect images that are part of the digital Vatican library project [5].Digital images can be manipulated in such a perfect way that the forgery cannot be visually perceived by naked eye. Nowadays, in our society, we can come in contact with a lot of tampered images, in news report, business, law, military affairs, academic research. More particularly, tampered images could be used to distort the truth in news reports, to destroy someone's reputation and privacy, e.g. by changing a face of a person in a photo with someone else's face. Law enforcement today uses emerging technological advances in the investigation of crimes. In fact Image Forensics technique is used mainly when an image is presented as an official proof to influence the judgment. During last decade different techniques for validating the integrity of digital images have been developed. Rest of this paper is organizes as follows In Section II describe the process of image forgery. In section III discuss the related work. In section IV discuss the problem formulation in section V discuss approach used for image forgery detection and finally discuss conclusion & future work in section VI.

II. IMAGE FORGERY TECHNIQUE

In this section discuss the image forgery technique. The image forgery technique is bucket of image tampering using any process of modification. Some very famous technique such as image enhancement, image painting, copy-move and image retouching. Some technique describe here.

a. Copy-Move Forgery

Copy move is the most common image tampering technique used due to its simplicity and effectiveness, in which parts of the original image is copied, moved to a desired location and pasted. This is usually done in order to hide certain details or to duplicate certain aspects of an image. Textured regions are used as ideal parts for copy move forgery, since textured areas have similar color and noise variation properties to that of the image which are unperceivable for human eye looking for inconsistencies in image statistical properties. Blurring is usually used along the border of the modified region to lessen the effect of irregularities between the original and pasted region.

b. Image Retouching

Image retouching is another class of forensic methods that pertains to a slight change in the image for various aesthetic and commercial purposes, not necessarily conforming to the standards of morality. The retouching is mostly used to enhance or reduce the image features. Usually this type of forgery is realized by changing the color or texture of the objects, intensify the weather conditions or simply introducing some blur for defusing the objects. The Image retouching has long been the norm in commercial photography, usually for photo-sessions, as

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

well as a routine in the showbiz industry. This type of forgery is also known as the image enhancement for its use to improve facial features. We also see some of the film industry stars refusing to allow retouching of some of their features Forgery detection, in case of image retouching, involves finding the enhancements, blurring, illumination and color changing.

c. Image splicing

Image splicing involves replacing of image fragments from one or more different images on to another image. Image splicing is one of the simple and commonly used image tampering schemes. Image splicing detection is of the fundamental task in image forgery detection. The method based on bispectral an analysis to detect un-natural higher-order correlations introduced into the signal by the tampering process and is successfully used for detecting human-speech splicing. An image has always implied the truth of what it represents. The advent of digital pictures and relative ease of digital image processing makes today this authenticity uncertain. The same tools, used to crop an image, eliminate "red-eye" or simply improve an image, can also be used to doctor images with despicable intent, creating an image that is not a representation of the reality

III. RELATED WORK

In this section discuss the related work in the field of image forgery detection. Some image forgery detection technique based on pixel based operation and some technique based on transform based technique.

[1] Here, Author presents in this paper, a scheme to detect the copy-move forgery in an image, mainly by extracting the key points for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to key point extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, they find the suspicious pairs of patches that may contain copy-move forgery regions, and they roughly estimate an affine transform matrix. In the second stage, an Expectation-Maximization-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy move forgery.

[2] In this paper They introduce a very novel hybrid approach, which compares triangles rather than blocks, or single points. Interest points are extracted from the image, and objects are modeled as a set of connected triangles built onto these points. Triangles are matched according to their shapes (inner angles), their content (color information), and the local feature vectors extracted onto the vertices of the triangles. Their methods are designed to be robust to geometric transformations. Results are compared with a state-of-the-art block matching method and a point-based method.

[3] Author Here propose a new algorithm for the accurate detection and localization of copy–move forgeries, based on rotation-invariant features computed densely on the image. Dense-field techniques proposed in the literature guarantee a superior performance with respect to their keypoint-based counterparts, at the price of a much higher processing time, mostly due to the feature matching phase. To overcome this limitation, they resort here to a fast approximate nearest-neighbor search algorithm, Patch Match, especially suited for the computation of dense fields over images.

[4] Author in this paper introduce As one of the most successful applications of image analysis and understanding, digital image forgery detection has recently received significant attention, especially during the past few years. At least two trend account for this the first accepting digital image as official document has become a common practice, and the second the availability of low cost technology in which the image could be easily manipulated. Even though there are many systems to detect the digital image forgery, their success is limited by the conditions imposed by many applications.

[5] Author introduces in this paper the growth of networked multimedia systems has magnified the need for image copyright protection. One approach used to address this problem is to add an invisible structure to an image that can be used to seal or mark it. These structures are known as digital watermarks. In this paper they describe two techniques for the invisible marking of images. They analyze the robustness of the watermarks with respect to linear and nonlinear filtering, and JPEG compression. The results show that their watermarks detect all but the most minute changes to the image. The proliferation of network multimedia systems dictates the need for copyright protection of digital property.

[6] Here author discuss A concise survey on the forgery detection methods was presented that may help researchers explore new ideas and provide new solutions to the challenges in the field, especially with blind methods. An attempt has been made to introduce various promising techniques that represent reasonable improvements in the forgery detection methods. Still these improvements are far from being perfect and have certain drawbacks that must be eliminated to obtain effective results. Specifically, the DCT- and PCA-based techniques, described in this survey, exhibit high computational complexity and do not possess effective accuracy rate.

[7] In this paper, they use manipulation of digital images has become easy due to powerful computers, advanced photo-editing software packages and high resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection and complete bibliography is presented on blind methods for forgery detection. Blind or passive methods do not need any explicit priori information about the image.

[8] Author discuss here In this paper Consistent decrease in cost of digital imaging hardware & increase in high quality user friendly image editing software for novice user has served variety of problems to society. Internet & social networking sites made it possible to host enormous no of images without provenance information or authenticity & made possible to share it with single click. Digital image

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

forensics is a research area trying to resolve the imposed problem of authenticity assuming that different imaging devices or processing would introduce uniform inherent patterns which are consistent in the original clean images and would become inconsistent after image manipulations.

IV. PROBLEM STATEMENT

In this section discuss some common problem related to image forgery detection some are discuss below

1. Data Provenance

The data provenance is necessary for protection of rights and may be regulatory requirement in applications like science, medicine, financial transactions government legal prosecutions and many more daily situations, wherever the information is valuable and trustworthy.

2. Benchmarking and Standard data set

There is need of open data sets for critical and typical realistic conditions such as images (digital documents) in uncompressed form with different resolutions, sizes and image acquisition model (camera model) with diverse contents for all possible forgeries such as copy-move, compositing, splicing, photomontage, blending, matting etc. with manipulation, and manipulation compensation conditions like adjustments color, contrast, brightness, blurring, enhancement and possible post suppression. The reason of the appearance of duplicate regions in an image is one of two things: first, the presence of two things or two objects with the same size, shape, and color; one of them may be a copy from the other one. Second, the presence of a relatively large area with one color and close in characteristics such as backgrounds (sky, wall, etc.) which leads to the appearance of duplicate regions in the results. Texture based image forgery detection have some limitation related the process of feature selection and region selection of coefficient block.

1. The major problem is measure the similarity of forgery and original image.
2. Optimal feature selection for the purpose of detection
3. Noise value of image equal to higher intensity value of actual image
4. Region of forged image are not precise

Most forged image are enhanced

V. CONCLUSION & FUTURE SCOPE

In this paper presents the review of image forgery detection technique and image forgery technique. The image forgery detection tool play impotent role in digital image forensics analysis. The transform based image of image forgery detection is very efficient in compression of pixel based operation. The transform based methods basically focus on texture based forgery detection. For the extraction of texture data from given image used various transform function such as SIFT transform, wavelet transform and many more transform function. The detection of transform based operation faced a problem of false negative and false positive value. In future used clustering technique for the minimization of negative and positive value.

REFERENCES

1. Jian Li, Xiaolong Li, Bin Yang, Xingming Sun “Segmentation-Based Image Copy-Move Forgery Detection Scheme” IEEE 2015 PP 507-518.
2. Edoardo Ardizzone, Alessandro Bruno, Giuseppe Mazzola “Copy–Move Forgery Detection by Matching Triangles of Keypoints” IEEE 2015 PP 2084- 2093.
3. Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva “Efficient Dense-Field Copy–Move Forgery Detection” IEEE 2015 PP 2284-2296
4. B.L.Shivakumar, Lt. Dr. S.Santhosh Baboo “Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods” Global Journal of Computer Science and Technology 2010 PP 660-664.
5. Matthew C. Stamm, K. J. Ray Liu “Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL-5, 2010. Pp 492-507.
6. Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, Cheng-Zhong Xu “Survey on blind image forgery detection” IET 2013 PP 660-669.
7. Gajanan K. Birajdar , Vijay H. Mankar “Digital image forgery detection using passive techniques: A survey” ELESEVIER Digital Investigation 2013 PP 226–245.
8. Archana V. Mire, Dr S. B. Dhok, Dr N. J. Mistry , Dr P. D. Porey “Catalogue of Digital Image Forgery Detection Techniques, an Overview” Elsevier, 2013 502-508.
9. Gung Polatkan, Sina Jafarpour, Andrei Brasoveanu, Shannon Hughes, Ingrid Daubechies “Detection Of Forgery In Paintings Using Supervised Learning”, 2012. Pp 12-17.
10. Yu-Feng Hsu ,Shih-Fu Chang “Detecting Image Splicing Using Geometry Invariants And Camera Characteristics Consistency”, 2012. Pp 341-344.
11. Gang Cao, Yao Zhao and Rongrong Ni “Edge-based Blur Metric for Tamper Detection” Journal of Information Hiding and Multimedia Signal Processing 2010.PP 20-27.
12. Chih-Chung Hsu, Tzu-Yi Hung, Chia-Wen Lin, Chiou-Ting Hsu “Video Forgery Detection Using Correlation of Noise Residue”, 2012.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.