International Journal of Science Technology and Management
Vol. No.4 Special Issue No. 01, August 2015
www.ijstm.com
ISSN 2394 - 1537

COMPREHENSIVE STUDY OF DIFFERENT TYPES IMAGE FORGERIES

G. K. S. Gaharwar[1, 2], Prof. V. V. Nath[3], R. D. Gaharwar[4]

[1]*Research and Development, Raksha Shakti University, Ahmedabad, (India)*

[2]*School of Business and Law, Navrachana University, Vadodara,(India)*

[3]*Institute of Management, Nirma University, Ahmedabad, (India)*

[4]*G. H. Patel Department of COMPUTER SCIENCE and Technology, Sardar Patel University, Vallabh Vidyanagar, (India)*

ABSTRACT

Image forgery means manipulating digital image to hide some important and key information from the image. Many times the forgery is done so meticulously that it is very difficult to identify the edited region from the original image. This papers surveys different types of active forgery techniques viz digital signature and digital watermarking and also different passive image forgeries viz copy-move forgery, image splicing, image retouching, and lighting condition.

s

Keywords: Digital Image Forgery, Active Authentication, Passive Authentication, Copy-Move Forgery, Image Splicing, Image Retouching, Lightning Condition

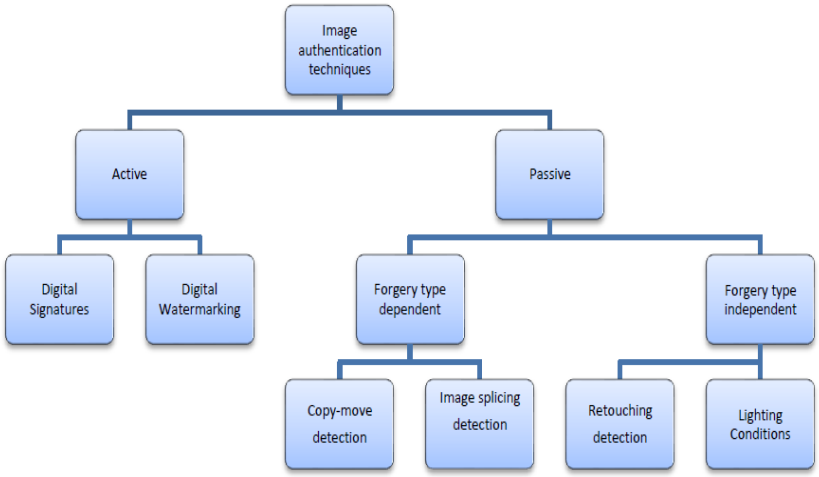
I. INTRODUCTION TO DIGITAL IMAGE FORGERY

Availability of low cost hardware and many advanced software tools has increased image forgeries in recent years. Moreover, these software works so well that it is very difficult to trace the forgeries in an image and so no image can be taken for granted for its originality. Due to this only images are not considered as evidence in the Indian legal system. Image forensics is a field of Digital forensics developed significantly to battle this problem and provide a tool to authenticate digital image.

II. CLASSIFICATION OF TYPES OF FORGERY AUTHENTICATIONS

For authentication of images several methods have been developed. These methods are broadly categorized into two classes: Active authentication and Passive authentication.

ISSN 2394 - 1537



III. ACTIVE AUTHENTICATION

In active authentication techniques prior information about the image is indispensable to the process of authentication. It is concerned 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 further classified into two types digital watermarking and digital signatures. Digital water marks are embedded into the images at the time of image acquisition or in processing stage and digital signatures embed some secondary information, usually extracted from image, at the acquisition end into the image. The main drawback of these approaches remains that they are to be inserted into the images at the time of recording using special equipments thus prior information about image becomes indispensable.

IV. PASSIVE AUTHENTICATION

Passive authentication also called image forensics is the process of authenticating images with no requirement of prior information just the image itself. Passive techniques are based on the assumption that even though tampering may not leave any visual trace but they are likely to alter the underlying statistics. It is these inconsistencies that are used to detect the tampering. Passive techniques are further classified as forgery dependent methods and forgery independent methods.

Forgery dependent detection methods are designed to detect only certain type of forgeries such as copy-move and splicing which are dependent on the type of forgery carried out on the image while as forgery independent methods detect forgeries independent of forgery type but based on artifact traces left during process of re-sampling & due to lighting inconsistencies. The main objective of passive detection technique remains to classify a given image as original or tampered. Most of the existing techniques extract features from image after that select a suitable classifier and then classify the features.

V. DIFFERENT TYPES OF IMAGE FORGERIES

Image forgeries are broadly categorized into,

5.1 Copy-move forgery

Copy-move is one of the most widespread image tampering technique, also it is very difficult to identify this type forgery as the copied image is taken from the same image. "In Copy-Move image forgery, a part of the image is copied and pasted to another part of the same image. It simply requires the pasting of image blocks in same image and hiding important information or object from the image."[HYPERLINK \l "Kau13" 1] This method involves copying of some area of an image superimposing it on some other area of the same image.

Image source[1]}

As the area copied belongs to the same image, the dynamic range and color remains will be same as the other part of image. Copy-move forgery is usually done to either hide some part of the image of to show some part of the image multiple times. Copy-move forgery detection aims at detecting the same or extremely similar areas and a lot of methods have been proposed to solve this problem. Generally, these detection methods are summarized into two categories: block matching-based and point matching-based. When creating a Copy-move forgery, it is often necessary to add or remove important features from an image. To carry out such forensic analysis, various technological instruments have been developed.

5.2 Image Splicing

"Image splicing is a technology of image compositing by combining image fragments from the same or different images without further post-processing such as smoothing of boundaries among different fragments." [HYPERLINK \l "Zha08" 2]

Image splicing forgery involves composition or merging of two or more images changing the original image significantly to produce a forged image. In case images with differing background are merged then it becomes very difficult to make the borders and boundaries indiscernible. Splicing detection is a difficult problem whereby the composite regions are investigated by a variety of methods. Abrupt changes between different areas that are combined and their backgrounds provide valuable traces to detect splicing in the image under consideration.

Image source [3]}

In order to get a large field of view image, we need to establish visual correlation among the images which were acquired by cameras placed at different locations. Via matching principle, we should com-pare the level of similarity between the target area and the same size area from the different search area in images, then we need to identify the position, where is the highest level of similarity. The position viewed as the best splicing position. Selecting two images from the images captured by cameras, then two sets of pixels were selected at intervals of a certain distance in horizontal direction, which is in the overlap of the first image. The gray ratio values of the two sets of pixels will be used as the reference template, and the best matching position from the overlap of the second image was searched. Because the gray values of some area in different images are close, if the reference template was selected improperly, it is easy to match wrongly.

5.3 Image Retouching

"In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative retouching." [HYPERLINK \l "Bur14" [4]]

Image is carried out to either reduce or improve certain features of the image. Retouching may require rotation, scaling, or stretching of an image before combining it with other image. It is very common type of image change and done very frequently commercials. Cloning of the part of the image is also very common in image retouching. The detection is very difficult as there is no radical change in the different parts of the image

Image Source:[4]}

One conservative view on retouching is that it is always an altering of reality, and that a retouched picture is not a "photograph" in the true sense of the word. On the one hand I can understand these purists, as a truly good photo needs hardly any edits, except perhaps for a contrast adjustment. On the other hand, ultimately, there is nothing despicable about retouching. Even in the days of film photography, retouching was one way to get rid of photo defects (dust, hair, etc.). Then as now, retouching was a process, a series of steps to improve a picture. For film, the steps most often included dodging, following by ink retouching (for black and white photos). In our digital age, retouching can mean practically any operation that somehow changes the feel of a picture—from use of a clone stamp to red eye correction to things like combining two pictures into one.

5.4 Lighting Condition

Now days the image forgery is very common where two movie stars are shown romantically involved. This type of forgery can be easily done by splicing two different images together. Often such spliced images are from different scene and having different lightning conditions and so it is very difficult for image forger to match exact lightning condition of one image with other. Such variation in lighting conditions can be used to identify the tempering in the image. "Many times the image splicing is done with such a precision that it is visually impossible to identify different lightning conditions in the combined image. To the extent that the direction of the light source can be estimated for different objects/people in an image, inconsistencies in the lighting direction can be used as evidence of digital tampering."[HYPERLINK \l "Joh05" 5]

As the combined tempered images are from different lighting conditions, the lightning condition of combined photograph might not be matching. This lighting inconsistency in the merged image can be used for the identification of image tampering. By approximating the direction of light source for different objects or people in an image, discrepancies in lighting are discovered in the image and alteration can be detected.

Image Source: [5]}

VI. CONCLUSION

Image forgery is a treat big threat as new and new tools are available with cheaper price for forging digital image. As there are many types of image forgeries, viz, copy-move forgery, image splicing, image retouching, and lighting condition, it is very difficult to have a image forgery identification techniques which applies to all

ISSN 2394 - 1537

types of forgeries. There are few forgeries like copy-move forgery, image retouching and image splicing, which are intentionally done with malafide intentions while use of lightning conditions is mostly done for enhancing image or to remove noise came due to bad image source of error while image capturing.

REFERENCES

[1] Amanpreet Kaur and Richa Sharma, "Optimization of Copy-Move Forgery Detection Technique," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, April 2013.

[2] Zhen Zhang, Ying Zhou, Jiquan Kang, and Yuan Ren, "Study of Image Splicing Detection," Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues, vol. 5226, pp. 1103-1110, 2008.

[3] Susama G Rasse, "Review of Detection of Digital Image splicing Forgeries with illumination color estimation," International Journal of Emerging Research in Management & Technology, vol. 3, no. 3.

[4] P. Sabeena Burvin and J. Monica Esther, "Analysis of Digital Image Splicing Detection," IOSR Journal of Computer Engineering, vol. 16, no. 2, pp. 10-13, Mar-Apr 2014.

[5] Micah K. Johnson and Hany Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," ACM Multimedia and Security Workshop, 2005.