ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Image Forgery & its Detection Procedure

Ashish Kumar Chakraverti
Research Scholar
IKG PTU, Jalandhar, Punjab India
ashish.me08@gmail.com

Prof.(Dr.) Vijay Dhir
Professor CSE
Jalandhar, Punjab, India
drvijaydhir@gmail.com

***Abstract:* - Image forgery and image forgery detection are emerging as well as hot research topics among researchers. In today's digital scenario, images are playing a major role in our day to day life and its manipulation is increasing exponentially. This manipulation is known as Image forging. In this review paper, we will study image forging, its types and detection process.**

Keywords: - Image forgery, Image forgery detection, Active technique, Passive technique, Digital Watermark, Digital Signature, Image Retouching, Image Splicing, Image Cloning

I. INTRODUCTION

With the introduction of digital technology, the use of images has increased in our day to day lives so as the forgery of digital images has become simpler, smart and indeterminable. 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 brand new door to the dark-side of it. We are living in an age, where something may be manipulated or altered with the assistance of advance technology. With the increasing applications of digital imaging, differing kinds of software programming tools are introduced for processing images and photographs. They are accustomed to build forge pictures to make it look realistic and sometimes objects may be added or deleted. For decades, images are used to document and they are used as proof in courts. Though photographers are able to produce composites of analog photos however this method is extremely time consuming and needs knowledgeable information thus it is arduous to implement than digital photos. Today, however, powerful digital image editing software packages makes image modifications easy [1]. Today's digital technology has begun to get rid of trust in our information, as from the magazines, to fashion world and in scientific journals, political campaigns, courts and also the picture that comes in our e-mail. All of these forged images are appearing with an additional frequencies and sophistication. The increase in the availability of multimedia information in digital form has come to a tremendous growth of tools to govern digital multimedia information contents.

The process developing fake image has been tremendously simple with the introduction of latest and powerful computer graphics editing software packages that are freely available as Photoshop, GIMP, and Corel Paint shop. In today scenario, this powerful image processing software's enable individuals to alter photos and pictures conveniently and in unseen manner. It creates an enormous challenge to authenticate pictures. Image forgery means manipulation of the digital image to hide some significant or useful data from it. Generally it is troublesome to spot the altered region from the first image. The detection of a forged image is driven by the requirement of authenticity and to maintain integrity of the image. The survey has been done on existing techniques for forged image and it highlights numerous copy–move detection and splicing detection ways based on their robustness and computational complexity [2].

Image forgery techniques are divided into two major categories: active and passive forgery. Active method requires some preliminary data of an image and such methods are not useful while handling images from unknown sources. This is biggest drawback of active method. Digital watermarking is one of them. Passive method does not need any preliminary data of digital image. The method works purely by analyzing binary information of digital image without any external information. Copy-move forgery belongs to this method [3]. Example of image forgery is shown below:

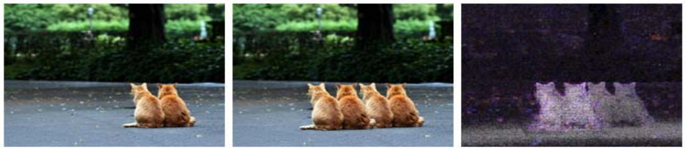


Fig. 1(a) Fig. 1(b) Fig. 1(c)

Figure1: Example of Copy-Move Image Forgery. 1(a) Shows Original Image 1(b) shows tampered image 1(c) Shows detection of tampered image

II. CLASSIFICATION OF IMAGE FORGERY TECHNIQUES

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

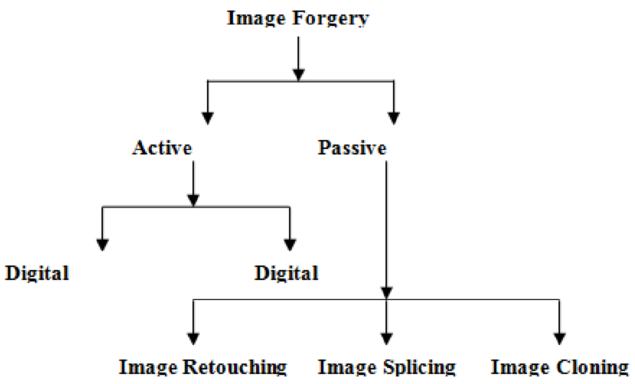


Figure .2: Shows Types of Image Forgery

A. Active Image Forgery Technique

In this technique, the digital image requires some sort of pre-processing such as watermark embedded or signatures are generated at the time of developing the image. However, in practice this would limit their application to a major extent. Digital watermarking [4] and signature are two main active forging techniques, as something is embedded into images when they are developed. If some special information cannot be extracted from the image we have, it is detected by the software package tool that the image is tampered. Watermarking is such a method of active tampering, 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 present times, a variety of schemes are embedded for security of 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.

B. Passive Image Forgery Technique

Passive image forgery is usually a great challenge in image processing techniques. There is not a single or specific method that can treat all the cases, but we have numerous methods available that deals with a specific type of passive forgery. In passive tampering detection, the raw image based on various statistics and semantics of image content to localize tampering of image is analyzed deeply. Security features are not embedded in passive forgery detection techniques as in the case of active forgery images, so ith is 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. ACTIVE IMAGE FORGERY TYPES

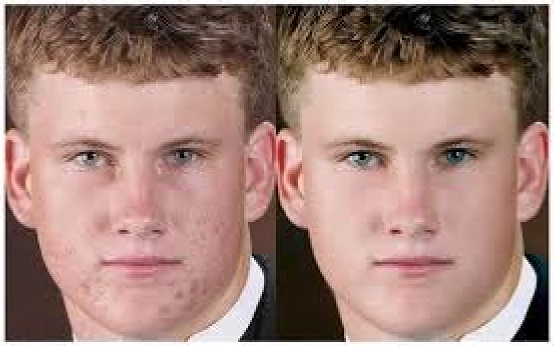
Digital Watermark: A digital watermark added to a photo, is more or less visible information in the form of a text or some other photo/image that has been added to the original photo. The added information can be more or less transparent to make it either easy or hard to notice the watermark.

Digital Signature: A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

IV. PASSIVE IMAGE FORGERY TYPES

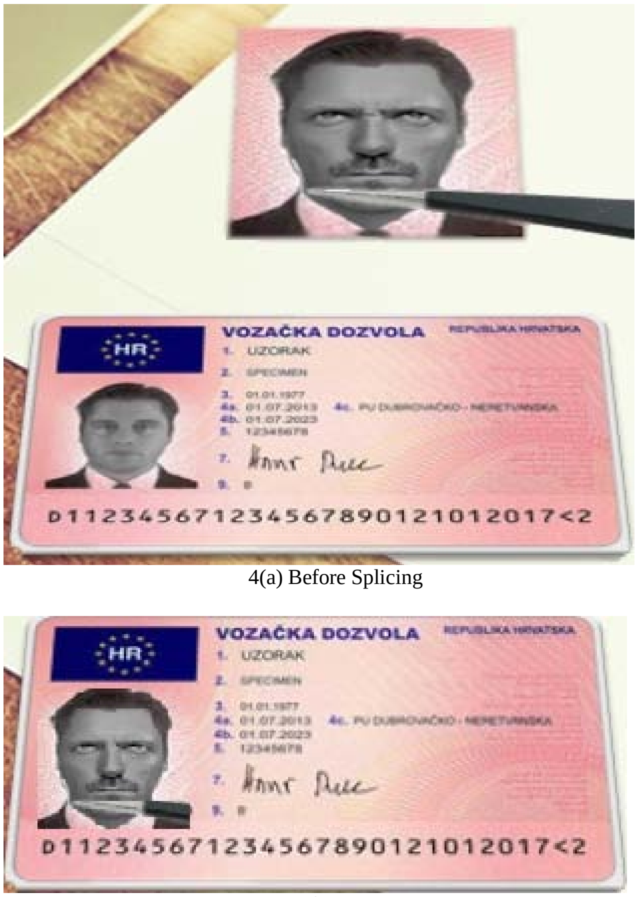
Image Retouching*:* Image Retouching is considered as less harmful kind of digital image forgery than other types present. In case of image retouching original image does not significantly changes, but there is enhancement or reduces certain feature of original image. This technique is popular among magazine photo editors they 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.



3(a) Before 3(b) After

Figure 3: Shows an example of Image Retouching.

Image Splicing (Copy-Paste or Photomontage): This technique for making forgery images is more common 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. 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 an identity proof which is forge image.

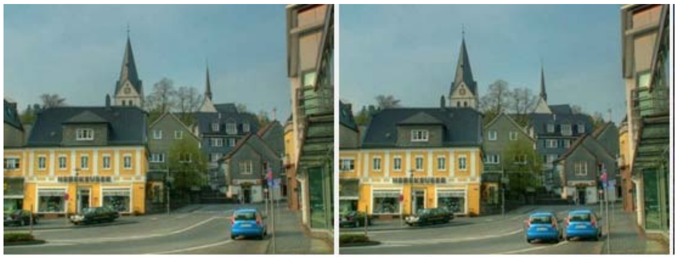


4(a) Before Splicing

4(a) After Splicing

Figure 4: Shows an example of Image Splicing

Image Cloning (Copy-Move): 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 [6]. The example of Copy-Move type is as shown below.



5(a) Before Cloning 5(b) After Cloning

Figure 5: Shows an example of Image Cloning

V. IMAGE FORGERY DETECTION

Active Image Forgery: Hidden Information inside the Digital Image is detected using software tools. This type of forgery is done at the time of data acquisition or before disseminated to the public. Embedded information can be used to identify the source of such image or to detect possible modification to that image.

Passive Image Forgery: It Use traces left by the processing steps in different phases of acquisition and storage of digital images. These traces can be treated as a fingerprint of the image source device. Passive methods work in the absence of protecting techniques. They do not use any pre-image distribution information inserted into digital image. They work by analyzing the binary information of digital image in order to detect forgery traces, if any

Its Limitation is the number of false positives.

Conclusion and Future Scope

In this review papers we studied image forging, its types in detail i.e. active and passive image forging. We also studied further classification active and passive types i.e. digital watermark, digital signature, image retouching, image splicing, image cloning. After that we studied active and passive image forging detection procedure in brief.

Based on detection procedure, we can implement existing algorithms and by analyzing that in detail we can also invent some new algorithms in the field of image forgery detection.

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 In-formation Hiding, Toronto, Canada, 2004.

[3] S. Kumar, P. Das, and S. Mukherjee, "Copy-Move Forgery Detection in Digital Images: Progress and Challenges," International Journal on computer Science and Engineering, vol. 3, no. 2, 2011, pp. 652-663.

[4] W.N. Lie, G.S. Lin, and S.L.Cheng, "Dual Protection of JPEG Images Based on Informed Embedding and Two- Stage 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%2F978-3-642-30157-5_71

[6] 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 .

[7] E. Lin, C. Podilchuk, E. Delp, "Detection of image alterations using semi-fragile watermarks," Proc. SPIE, Security and Watermarking of Multimedia Content II, vol. 3971, 2000, pp. 152–163.

[8] Gajanan K. Birajdar, Vijay H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital Investigation, vol. 10, no.3, 2013, pp. 226-245.

[9] O. M., Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art," Forensic Science International, vol. 231, no. 1, 2013, pp. 284–295.

[10] J. Fridrich, D. Soukalm, J. Luka ́s ˇ, "Detection of copy-move forgery in digital images," Digital Forensic Research Workshop, Cleveland, OH, 2003, pp. 19–23.

[11] A.C. Popescu, H. Farid, “Exposing Digital Forgeries By Detecting Duplicated Image Regions,” Tech. Rep. TR2004-515, Dartmouth College, 2004.

[12] Ashima Gupta, Nisheeth Saxena, S.K Vasistha, “Detecting copy move forgery using DCT”, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153 .

[13] B. Mahdian and S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants,” Forensic science international, vol. 171, no. 2, 2007, pp. 180–189.

[14] K. S. Bacchuwar and K. Rama krishnan, “A Jump Patch-Block Match Algorithm for Multiple Forgery Detection,” International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing,2013, pp. 723-728.

[15] R.C. Gonzalez, R.E. Woods, “Digital Image Processing”, 2nd edition, Addison- Wesley, 2003.

[16] V. Christlein, C. Riess, J. Jordan, C. Riess, E. Angelopoulou: "An Evaluation of Popular Copy-Move Forgery Detection Approaches, "IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, 2012, pp. 1841-1854

[17] 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.

[18] 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.

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

[20] 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.

[21] Pradyumna Deshpande, Prashasti Kanikar, “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.

[22] 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.

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

[24] 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.

[25] Zhang J, Feng Z, Su Y. A new approach for detecting copy-move forgery in digital images. 11th IEEE Singapore International Conference on Communication Systems (ICCS '08); November 2008; pp. 362–366.

[26] Dhir, Vijay. "Alchemi.NET Framework in Grid Computing." Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development at Bharati Vidyapeeth’s Institute of Computer Applications and Management, New Delhi. 2009.

[27] Dr. Vijay Dhir, Er. Gagandeep Kaur ,”Execution of cloud using freeware Technology” , International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol 3, Issue 12, pp 22-29, December 2016.

[28] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, “Grid Job Scheduling - A Detailed Study”, International Journal of Innovative Research in Science, Engineering & Technology Vol.2, Issue 10, October 2013.

[29] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, “Nimble@ITCEcnoGrid Novel Toolkit for Computing Weather Forecasting, Pi and Factorization Intensive Problems”, International Journal of Computer Engineering & Technology (IJCET) , Vol:3 Issue:3, Dec 2012.

[30] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, “Computational Grid based on Alchemi.NET framework”, International Conference on Computer, Electrical, and SystemsScience and Engineering, Feb 10, 2009 WCSET 2009: World Congress on Science, Engineering & Technology Hong Kong March 23-25, 2009.

[31] Vijay Dhir, Ashish Kumar Chakraverti, and Sugandha Chakraverti, “Architectural and Qos Issues in Mobile Cloud Computing Environment for Real-Time Video Streaming”, International Journal of Advanced Computer Science and Applications ISSN: 2158-107X (P), 2156-5570 (O), Vol. 7, No. pp: 355-366, January2016