ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# *Review Paper on Re-Sampling Detection in Digital Image Forensics Using Peak Value Identification Classifier*

**Amaninder Kaur**[1]
Student, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib - India

**Sheenam Malhotra**[2]
Assistant Professor, CSE Department
Sri Guru Granth Sahib World University
Fatehgarh Sahib - India

***Abstract:*** ***The availability of photo manipulation software has made it unprecedentedly easy to manipulate images for malicious purposes. One of the most common forms of digital image or photographic manipulation operation is known as image resampling, which is generated by geometric transformations like a resizing and/or rotation. Resampling introduces specific correlations in the image samples, which can be used as an evidence of editing. These correlations may not be visible to a human, but can be detected by statistical techniques. This paper presents a Supervised Learning Technique for Re-Sampling Detection in Digital Image Forensics using Peak Value Identification Classifier.***

***Keywords: Digital Image Forensics, Digital Image Forgery, Digital Image Forgery Detection Techniques, Resampling Detection, Support Vector Machine, Peak Value Identification Classifier.***

## I. INTRODUCTION

In today's world Digital Image Forensics is highly challenging field. Digital Image Forensics is a relatively new research field aiming at gathering information on the history of an image in such a way that its authenticity can be evaluated. With the proliferation of digital images and powerful image editing tools such as Photoshop, it has become increasingly easy to manipulate images to alter content and meaning. Different types of software are introduced for image processing. Such software can do an alteration in digital image by changing blocks of an image with no showing the effect of the modification in the forged image. The extent of emerging new techniques of forgeries is increasing regularly. To find out the forgery, the images go through some forensic image processing. Specifically image forensic includes the alterations of pixel values only. Mainly Digital image forgery detection techniques are classified into active and passive approaches. In the active approach, the digital image requires some preprocessing such as watermark embedding or signature generation at the time of image acquisition; it is mainly based on the watermark computation by the camera. In contrast to active approaches, passive techniques operate without any requirement of watermarks or signature embedded in advance. These techniques work on the notion that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of the image. It can be grouped into five categories:

a) Pixel- based techniques

b) Format- based techniques

c) Camera- based techniques

d) Physical Environment -based techniques

e) Geometry-based techniques.

In pixel based detection different image forgeries are copy-move (cloning), resampling, splicing and retouching. In this work main focus on detecting a common type of digital image forgery called resampling forgery. Users very often apply to

© 2015, IJARCSMS All Rights Reserved 

image geometric transformations like a resizing and/or rotation. Since objects in images are often on different scales, resampling is necessary to create a visually convincing forgery. These operators apply in the pixel domain, affecting the position of samples, so the original image must be resampled to a new sampling lattice. Resampling introduces specific correlations in the image samples, which can be used as an evidence of editing. For example making a composite of two people it might be possible that one person may have to be resized, stretched to match the relative height of other people. So this process needs to resample original image into a new sampling lattice. Resampling detection techniques can be exploited for detecting both benign editing (e.g., scaling or rotation of the whole image) as well as malicious editing (by checking if only a certain region has been resized, thus altering the information carried by the image). Resampling also affects the display size of image. When sample is down, meaning that decrease the number of pixels in image, information is deleted from the image. When sample is up, or increase the number of pixels in your image. New pixels are added based on color value of existing pixels.

Below Fig. 1 shows the example of image resampling, in which resampling pixels that make up the dog's eye.

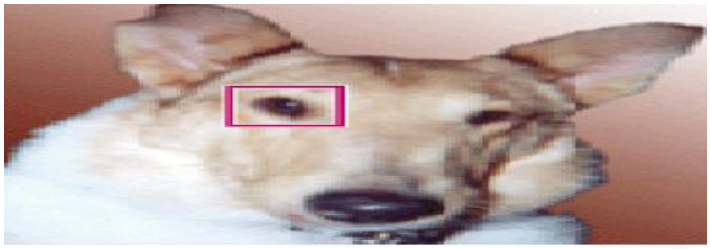

Fig. 1 Exampleof Image Resampling

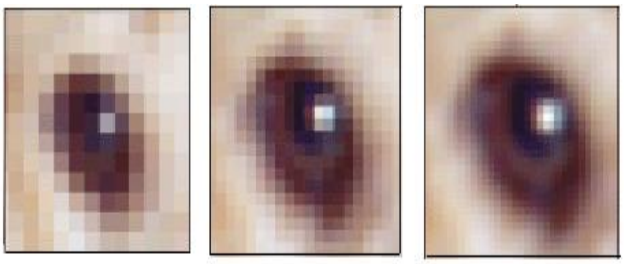

Fig. 1 (A) Down sampled

Fig. 1 (B) Original Sample

Fig.1 (C) Up sampled

In above Fig. 1 (A) shows down sampled, Fig. 1 (B) shows original sample and Fig. 1(C) shows up sampled. Therefore by having a reliable technique to detect the resampling forgery will be able to detect forgeries that contain among others this type of tampering. For this purpose, in digital image forensics a supervised technique will be implement using peak value identification classifier in this paper.

## II. Literature Review

The following literature provides the outline of work carried by various authors about Resampling Detection in Digital Image Forensics:

**Ali Qureshi and M. Deriche [1]** presented that with the advent of powerful image editing tools, manipulating images and changing their content becoming a trivial task. It is now possible to add, modify, or remove important features from an image without leaving any perceptual traces of tampering. To this end, image forensics techniques aim at restoring trust and acceptance in digital media by uncovering tampering methods. Such detection techniques are the focus of this paper. In particular, provide a survey of different forging detection techniques with a focus on copy and move approaches.

**A. Popescu and H. Farid [2]** presented the Popescu and Farid's EM algorithm for learning correlations between pixels was implemented. An SVM classifier was trained to determine if the correlations found by the EM algorithm result from re sampling. This classifier was shown to have better performance than the KNN classifier at low resampling rates and does not require an exhaustive database of synthetic maps.

**P. Sabeena Burvin, P.G. Scholar and J. Monica Esther [3]** presented a several methods proposed to detect image composition to insist the necessity for image splicing detection. This field is still growing and a lot of research is needed to make digital forensic more promising. To identify such kind of image manipulations, many researchers have been carried out on image splicing. But the existing methods of detecting image splicing undergo the following challenges: original image is essential for revealing tampering, forgeries with indoor image and image resolution.

© 2015, IJARCSMS All Rights Reserved 

**P. Subathra, A. Baskar and D. Senthil kumar [4]** presented a resampling technique using automatic selection of region of interest method. The proposed method is based on a statistical approach. This technique is easily detecting the traces of tampering region of scaling, rotation, skewing transformations, and any of their arbitrary combinations in image. This method is fast, blind, and efficient. It works for a wide variety of resampling factors or rotation angles.

**P.G. Gomase and N.R. Wankhade [5]** presented a classification of Image forgery detection techniques. A technique for copy-move forgery detections is discussed. But this approach takes into account only shifting of copied regions. So another technique is discussed for fast-copy-move detection. Basic design and algorithm of proposed system is on the basis of above mentioned techniques. First technique i.e. copy move forgery has lower computational complexity but the final result is not precise, on the other hand second approach is complex but precise.

**Sanawer Alam and Deepti Ojha [6]** presented the various image manipulation techniques. New technique in the forensic as well as in the anti forensic field is discussed. Manipulation of digital media was almost impossible hardly 20 years ago, which is quite common now a day. Although, very efficient techniques are available to detect tampering, even then the number of tampering is also increasing. Undoubtedly, processing information can be finding out by using these techniques for a manipulated image, but the fact is that an expert can do undetectable manipulations in the image. All these demand for a new technique in the forensic as well as in the anti forensic field.

**Kusam, Pawanesh Abrol and Devanand [7]** presented the techniques and methodologies for validating the authenticity of digital images and testing for the presence of tampering and manipulation operations on them have recently attracted attention. Detecting forgery in the digital images is one of the challenges of this exciting digital age. As a result, the authenticity of images can't be taken for granted, especially when it comes to legal photographic evidence.

**A. Meenakshi Sundaram and C. Nandini [8]** presented the essentials of image forensics and various techniques used for detection of forged part of the image. The study has discussed image retouching, image splicing as well as copy move attack as majority of the literatures considers such types of image attacks. From the study it was evident that all such categories of image forgery technique have their potential adversarial feature depending upon the scale of vulnerability of the victim. The paper has also discussed about the forgery detection techniques, where multiple standard techniques were discussed.

**E. Abhitha and V.J. Arul Karthick [9]** presented a set of forensic operations capable of finding compression fingerprints from digital images. In this paper, developed a generalized framework for the removal intrinsic fingerprints from an image's transform coefficients and developed an algorithm that identifies the anti-forensic effect. Anti forensics is capable of fooling forensic techniques. An anti-forensic operation leaves behind its own unique fingerprints, a new forensics detection technique can be designed by using this fingerprints.

**A. Popescu and H. Farid [10]** presented various algorithm formed by Popescu and Farid's for exposion of forgeries in digital image. The different algorithm will be derived to find the forgeries which are generated in digital image because of interpolation due to factor color filter array.

## III. PROPOSED WORK

In a resampled image, certain pixels are linear combination of its neighbors. These pixels are correlated with its neighbors and will appear periodically in the resampled image. For detection of resampling, will be going through each pixel and obtaining the results by following steps:

**Step 1:** Find out its neighbors in a certain window size of 2N+1**,** if pixels are resampled matrix is also resampled. Due to the periodic correlations between resampled pixels, resampling matrix is periodic. Neighboring pixels can be also naturally correlated, so to detect the periodicity Fourier Transform is used and refer to magnitude of transform as periodic.

© 2015, IJARCSMS All Rights Reserved 

**Step 2:** To find out the periodicity, implement the KNN algorithm. Then train a support vector machine (SVM) to classify a periodicity map as resampled or non-resampled. There are different peak values for sampled and resampled values. The classifier must be able to distinguish between natural peaks in the periodicity map from those introduced by resampling.

## IV. Conclusion

Nowadays, image resampling image forgery is becoming a common way the anti-social people are using to create the fake photographs and misusing them. So it is necessary to identify such kind of image manipulations. With the current presented work, it is concluded there are many techniques for detection of resampling forgery in digital image. To detect this kind of forgery; a technique will be implemented using Peak Value Identification Classifier. With above mentioned work, it will be able to detect resampling with lesser blocks of testing sample and then as a result it will definitely reduce the time complexity, which will minimize the error rate.

## Acknowledgement

It is my pleasure to get this opportunity to thank my beloved and respected Guide Mrs. Sheenam Malhotra, Assistant Professor of Computer Science and Engineering, who imparted valuable basic knowledge related to Image forensics and thankful to Sri Guru Granth Sahib World University, Fatehgarh Sahib, which gives the opportunity to learn and spread the light of education.

## References

1. Ali Qureshi, M. Deriche, "A Review on Copy-Move Image Forgery Detection Techniques," Multi-Conference on Systems, Signals & Devices (SSD), 2014 11th International, pp.: 1, February 2014.
2. A. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling," IEEE Transactions on Signal Processing, vol. 53, pp.: 758 – 767, Issue No. 2, February 2005.
3. P. Sabeena Burvin, P.G. Scholar and J. Monica Esther, "Analysis of Digital Image Splicing Detection," IOSR Journal of Computer Engineering (IOSR-JCE), ISSN: 2278-0661, Vol. 16, pp.: 10-13, Issue No. 2, Ver. XI, April 2014.
4. P. Subathra, A. Baskar and D. Senthil kumar , "Detecting Image Forgeries using Re-Sampling by Automatic Region of Interest (ROI)," Ictact Journal on Image and Video Processing, ISSN: 0976-9102, Vol. 02, Issue No. 04, May 2014.
5. P.G. Gomase and N.R. Wankhade "Advanced Image Forgery Detection," IOSR Journal of Computer Science (IOSR-JCE), ISSN: 2278-8727, pp.: 80-83, April 2014.
6. Sanawer Alam and Deepti Ojha, "A Literature study on Image forgery," International Journal of Advance Research in Computer Science and Management Studies, ISSN: 2321-7782, Vol. 2, Issue No.10, October 2014.
7. Kusam, Pawanesh Abrol and Devanand, "Digital Tampering Detection ," BIJIT - BVICAM's International Journal of Information Technology and Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), ISSN: 0973 – 5658 , Vol. 02, December 2009.
8. A. Meenakshi Sundaram and C. Nandini, "Investigational Study of Image Forensic Applications, Techniques and Research Directions," International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol. 4, Issue No. 8, August 2014.
9. E. Abhitha and V.J Arul Karthick., "Forensic Technique for Detecting Tamper in Digital Image Compression," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue No. 3, March 2013.
10. A. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," IEEE Transactions on Signal Processing, Vol. 53, pp.: 3948-3959, Issue No. 10, October 2005.

## Author(s) Profile


**Amaninder Kaur** is a student of M.Tech (CSE department), Sri Guru Granth Sahib World University Fatehgarh Sahib, India.


**Mrs. Sheenam Malhotra** is assistant professor of CSE department, Sri Guru Granth Sahib World University Fatehgarh Sahib, India

© 2015, IJARCSMS All Rights Reserved 