Highlighting Image Tampering Using Statistical Quality Evaluation

Surbhi Gupta[1], and Parvinder Singh Sandhu[2]

***Abstract*---**With the advancement in information technology and image processing software the manipulation of the images is increasing considerably from past years. Therefore, Image tampering is gaining research interest. Many manipulation and hence detection techniques exists. This paper aims at comparing and discussing various statistical based approaches utilized for image forensics.

Keywords—Image Tampering, Image Manipulation, Copy Move, Noise inconsistency, quality metrics, statistical evaluation

I. Introduction

WITH the advancement in information technology and image processing software the manipulation of the images is increasing considerable from past years. These manipulations can be as simple and harmless as editing one's individual pictures and may be as crucial and harmful as editing a crime scene. The main reason behind the popularity of image and its processing software is mainly because what we see is what we believe. Images have been widely used as an evidence for some event or happening for long. Retouching of the images has been so popular that nowadays one can hardly believe their authenticity. Retouching may be done for enhancement purpose by keeping the contents of the image intact or for creating forged images by intentionally altering the contents. Enhancement based retouching does not matters much but intentionally created forged images may cause several problems when presented in the court of law. The obvious reason includes extensive use of internet which is the main source of images as well as image processing software and lack of law enforcement in such cases. Even an amateur can create forged images for playful purpose. Moreover these processing software do not leave any traces of forgery. Post processing further makes the revealing task difficult.

Image forgery has a long history [1]. Due to problems mentioned above a whole community of researchers are devoted to work in this field. It is very evident as the number of paper publications in this field is rising enormously. Different image forgery techniques and their detection have been reported by various authors till date. Various section of this paper is as follows. First section has classification of image forgery types. Second section has the classification of various forensic techniques. Then the statistical evaluation based techniques of image forensics are categorized and discussed. A comparison of these techniques is presented so that it may serve as a guide for the researches working in this area.

II. Image Manipulation Techniques

Image manipulation is done usually for some specific purpose. It may be done to hide some content from the image or to alter the contents by combining it with other images. Many such methods are prevalent among the forgers. Most common of them have been copy move and splicing.

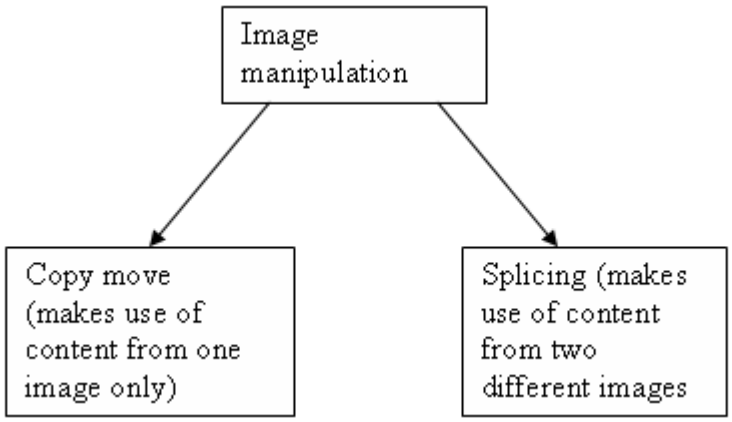

Fig. 1. Image manipulation types

[1] Research Scholar, I. K. Gujral Punjab Technical University, Jalandhar
[2] Research Guide, I. K. Gujral Punjab Technical University, Jalandhar

Copy move forgeries [2] are usually done to hide some content from the original image. It is named for manipulations where a part of the image is taken, may or may not processed and then moved and pasted into the same image. It usually follows four steps. First a patch from the original image is taken which is believed to be replicated semantically by cropping. Then some image processing operation like scaling, rotation is applied to make it look different from the original patch. Then is patch is moved i.e. translated in the image and then pasted onto the area which the user wanted to hide.

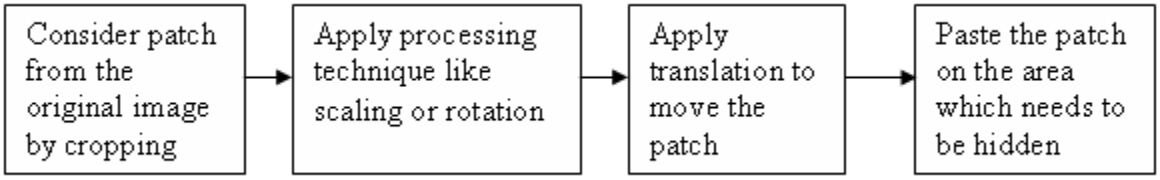

Fig. 2. General method followed for copy move forgery

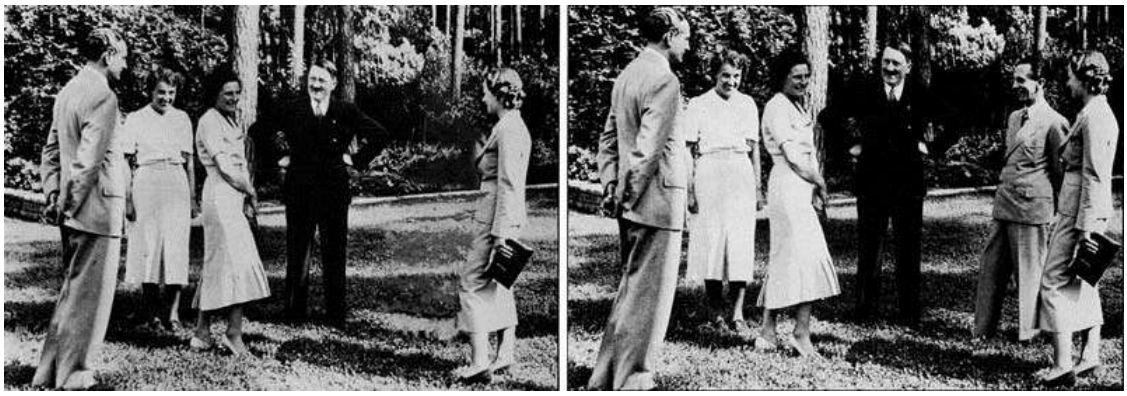

Fig. 3. Hitler Removes Joseph Goebbels, 1937
In this doctored photograph we see Joseph Goebbels removed by Hitler. [Source: fourandsix.com]

Splicing is done for create a false impression by displaying the contents taken from two or more images together [3]. It is named for manipulations where a part of image is taken from one image, may or may not be processed and then moved and pasted into a different image. Contents from more than two images may also be considered. It usually follows four steps. First a patch from image other than original is taken by cropping. Then some processing technique like scaling, rotation, brightness & contrast adjustment or sharpening & blurring is applied on the patch to match its appearance with the original image. This patch is then moved and pasted in the original image to create a false impression.

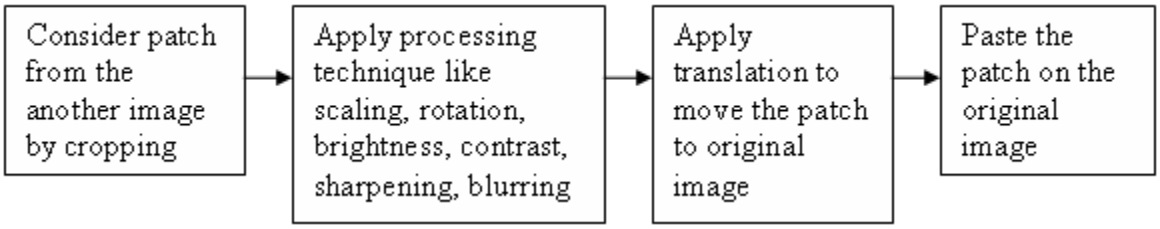

Fig. 4. General method followed for splicing

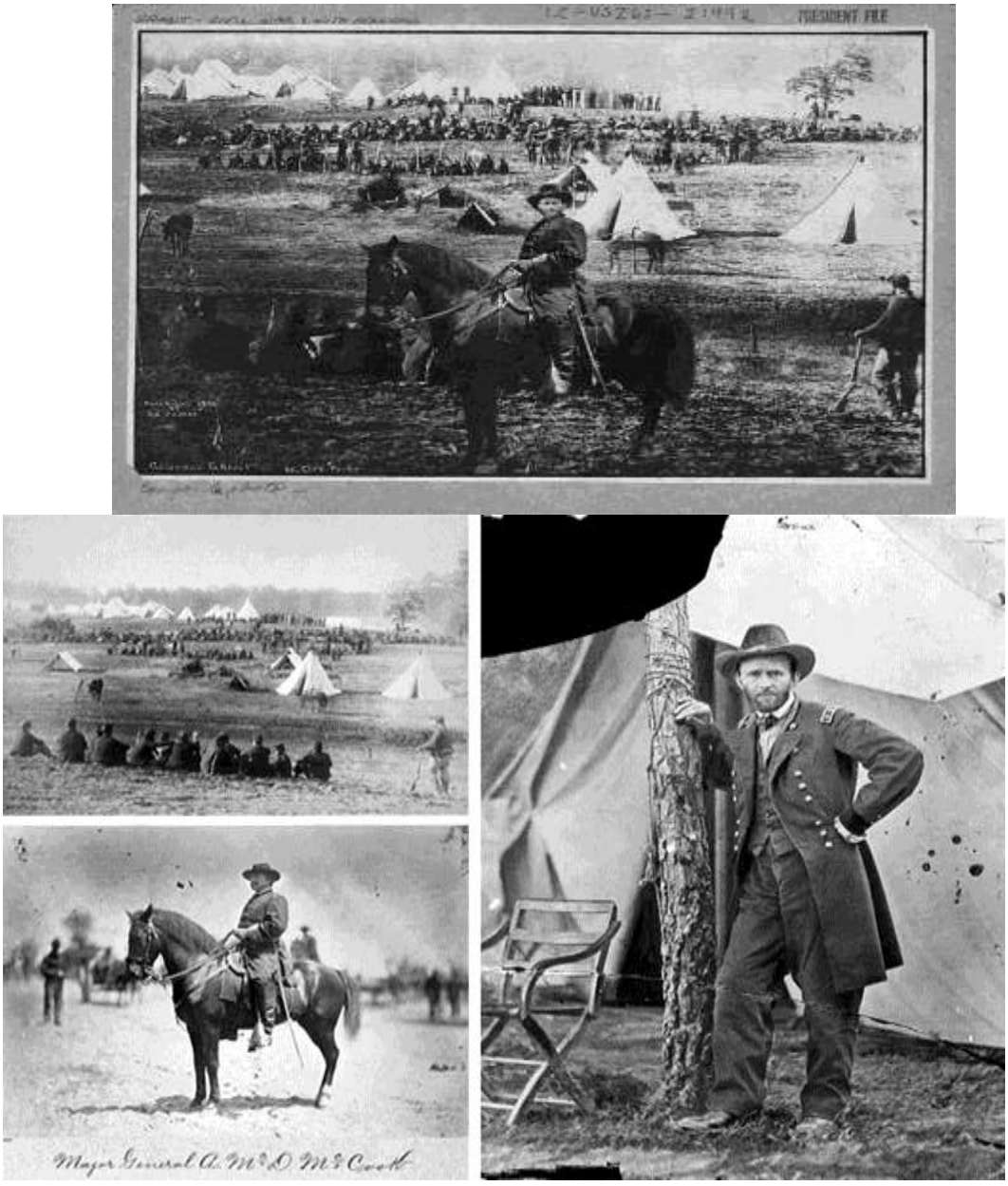

Fig. 5. General Ulysses. S. Grant on a Horse in front of Troops, circa 1864

Researchers at the Library of Congress uncovered this image which appears to show General Ulsses S. Grant in front of his troops at City Point, Virginia during the American Civil War. Investigation proved that the image to be made of three separate prints: the head is taken from a portrait of Grant; the horse and body are those of Major General Alexander M. Cook; and the background is of Confederate prisoners captured at the battle of Fisher's Hill, Virginia. [Source: fourandsix.com]

III. IMAGE FORENSIC TECHNIQUES

Image forgery detection methods are broadly classified as active and passive methods. Active methods are preventive whereas passive methods are reactive. Active methods use precautionary measures to prevent forgery of images by using digital signatures or watermarks. One can check the authenticity of the document anytime by checking the watermark or signature present on it. It's usually followed for official document and images to protect them from forgery. Usually a code is embedded in the image which can be checked later for ensuring its authenticity. But this method requires either hardware or software so its not possible to use them for each and every image clicked. Such images are equally prone to forgeries and need special methods to detect the traces of manipulations. These types of methods come under passive methods. Such methods are adopted when an image not protected by active methods is suspected for forgery. Passive methods are further classified as [4]

- Source based detection
- Tampering operation based detecting
- Statistical irregularities based detection
- JPEG compression based detection

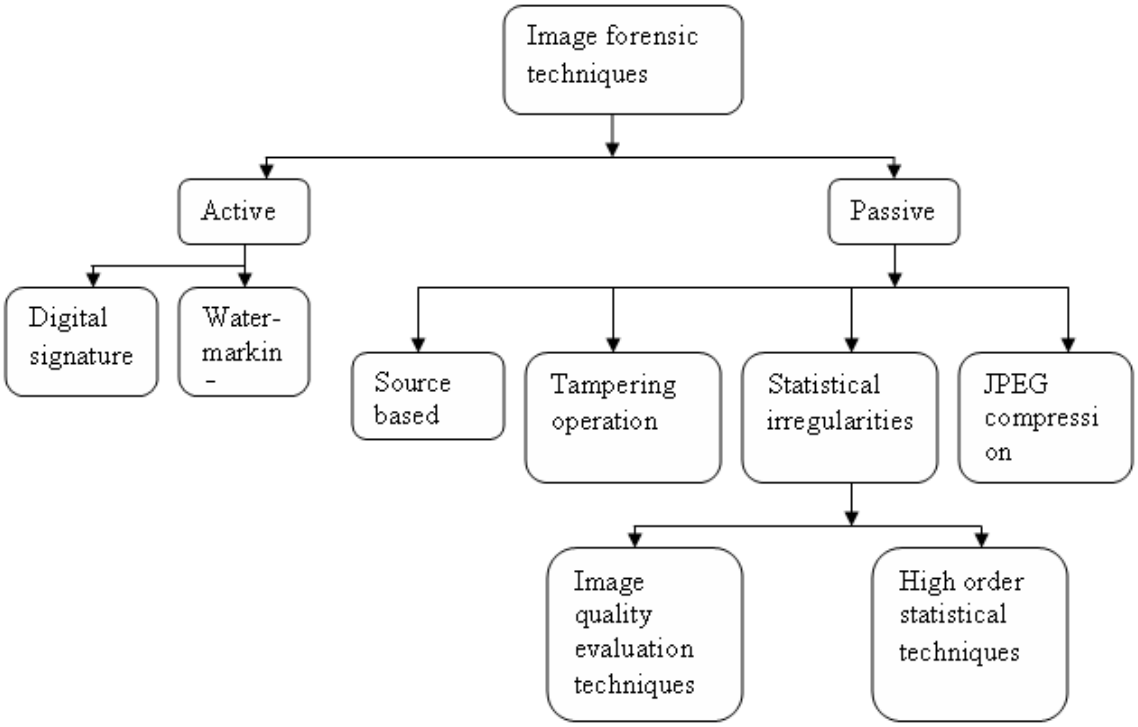

Fig. 6. Different approaches for forgery detection in images

IV. Statistical Forgery Detection

Xin li (2002) proposed blind image quality assessment without using reference images [5]. Proposed model works on three quantities: the edge sharpness level, the random noise level and the structural noise level. Mathematical tool is developed to transform the heuristics into noise structures under various circumstances. Accuracy of proposed measure increases credibility.

Avcibas et al. (2004) conducted a statistical analysis of image quality measures which reveal different perspectives of image [6]. Author applied them to reveal compression and steganography. Further author selected four measures from the list of image quality measures i.e. two first-order moments of the angular correlation and two first-order moments of the Czenakowski measure. They used a training set of original images and their manipulated versions. A linear regression classifier was then designed using the statistics collected. The accuracy achieved was 91% if manipulation operation is applied on whole image and is 80% if manipulation is applied on small regions of image.

Popescu in [2004] has given a method for detecting manipulation based on noise [7]. Author developed a blind estimator to measure the local noise variance in an image. First the image is segmented into overlapping blocks and then the noise variance is estimated for each block. According to the model if image has two or more different levels of noise the probably if its being tampered increases.

Fu et al. (2006) applied Hilbert Huang transform to generate statistical model based on moment of characteristics functions with wavelet decomposition [8].

Bayram et al.(2006) validated the images based on three different forensic features based on Image quality metrics, multi-scale decompositions, correlation and texture properties [9]. The statistical tool named as Binary Similarity Measures (BSM) is introduces which is based on correlation and texture characteristics between the bit planes. Then it is combined with existing models of Image Quality Measures and High order Wavelet Statistics.

Gou et al in his paper [2007] performed statistical noise feature extraction using denoising algorithms [10]. Three difference aspects of noise are studied. These are based on de-noising algorithms, wavelet analysis and neighborhood prediction. De-noising algorithm based on averaging, gaussian, median and wiener filtering are used. After that 2 features per channel are extracted to extract 30 features. Mean and standard deviation of log of pixel difference is taken as statistical feature. Then high frequency sub bands are used. Mean and standard deviation of wavelet coefficient are taken as statistical features. The two statistical featured based on mean and standard deviation of neighborhood prediction are taken. Total 60 features are extracted and then classification of original and tampered image is done using support vector machines. The classifier is proved to be 90% efficient id distinguishing direct camera outputs from tampered versions. Moreover the same classifier can also detect steganography operations on the image so the algorithm provided a general framework which must be followed

when type of operation performed for tampering are not known.

Zhang et al. (2008) proposed a splice detection method based on multi-size block discrete cosine transform and image quality measures [11]. Their model measures statistical differences between original and fake image. Author demonstrated the efficiency of the model and its broad application domain.

Ryu et al (2008) has developed a classifier based on Avcibas image quality measures to utilize them for image forgery detection [12]. They considered 3 measures to represent pixel differences, 5 measures to measure similarity between two images, 6 measures from frequency domain, 3 measures related to Human Visual System. SVM prints classifier is used for classification of image as genuine or fake. First the classifier is trained using original and fake documents for each quality measure. Author used one laser and one inkjet printed copy and one scanner. The SVM classifier is trained and tested with the data sets combination from both printers and scanner. The classifier achieved greater than 80% accuracy.

Mahadian and Saic (2009) in their paper proposed an algorithm for detecting tampering using noise inconsistencies [13]. Their algorithm segments the image on the basis of varying noise levels. They assumed white Gaussian noise for the experimentation. The main steps of the algorithm consist of block wise analysis of wavelet, followed by tiling sub band HH1, followed by noise variance estimation. Then the blocks are merged based on region merging techniques. Author used Median absolute deviation as estimator on sub band HH1. The algorithm works well in the presence of high noise degradations only. Moreover it may identify the regions of the image which are not manipulated due to their noise inconsistency. The main limitation of the algorithm is that it cannot be used as a standalone forgery detector rather supplements. It works well if a certain region of image is suspected for manipulation. Human interpretation is crucial for successful detection.

Stamm et al (2010) worked on statistical fingerprints for forensics detection [14]. The author proposed statistical intrinsic fingerprint measures for pixel value mapping, detecting contrast enhancement and detecting additive noise due to jpeg compression. Author claimed to achieve 99% probability of detection for fake images and 7% probability for false alarms. A model for original image pixel value histogram is proposed which is utilized for global and local contrast manipulation detection. Further histogram equalization fingerprints are utilized to detect cut and paste type forgeries.

Recently Liu and Pun (2015) in [15] has developed an algorithm for detecting noise discrepancies. This method segments the image based on objects and boundaries and then sharp areas need to be detected using Sobel operator and then dilation is applied so that these areas may not interfere during noise estimation later. De-noising is applied on the image followed by noise detection using five different filters. The mean and standard deviation is studied for each segment as a noise feature. Later energy based graph cut is used to label the regions as manipulated area and original area. Author demonstrated the efficiency of the algorithm in various scenarios.

TABLE I
COMPARATIVE ANALYSIS OF VARIOUS STATISTICAL METHODS FOR TAMPER DETECTION

Author	**Features utilized**	**Probability of detection**	**False alarms**
Xin li (2002)	Edge sharpness level, the random noise level and the structural noise level	Not mentioned	Not mentioned
Avcibas et al.(2004)	Two first-order moments of the angular correlation and two first-order moments of the Czenakowski measure	91% if manipulation operation is applied on whole image 80% if manipulation is applied on small regions of image	12% if manipulation operation is applied on whole image 28% if manipulation is applied on small regions of image
Popescu and farid (2004)	Correlation between each pixel and its neighbors, DCT coefficients & their histograms and signal to noise ratio	NA	NA
Fu et al. (2006)	HHT and moment of characteristics functions with wavelet decomposition	80.15%	NA
Bayram et al.(2006)	Image quality metrics, multi-scale decompositions, co-relation and texture properties.	90%	25%
Gou et al.(2007)	De-noising, wavelet analysis and neighborhood prediction	90%	5%
Zhang et al. (2008)	Multi-size block discrete cosine transform and image quality measures	87.10%	NA
Ryu et al (2008)	3 measures to represent pixel differences, 5 measures to measure similarity between two images, 6 measures from frequency domain, 3 measures related to Human Visual System	80%	NA
Mahdian and Saic (2009)	Block wise analysis of wavelet, followed by tiling sub band HH1, followed by noise variance estimation	NA	High false positives
Stamm et al. (2010)	Pixel value mapping, global and local contrast enhancement and additive noise	99%	3.7%
Liu and pun(2015)	Edge based and de-noising	100% for high ISO	NA

V. CONCLUSION

Passive or blind techniques and methodologies for validating the integrity and authenticity of digital images is one of the rapidly growing areas of research. Passive methods require no extra prior knowledge of the image content or any embedded watermarks or signature. This paper presented overview of methods for statistical digital image tampering detection. Different image forgery detection techniques are categorized and their feature base and performance is presented in this paper. Most of the techniques are developed to detect image tampering able to localize the forged areas but all of them have the disadvantage of false positives. We hope this work will help the researchers working in the field of digital image forgery detection.

REFERENCES

[1] A. Rocha , W. Scheirer, T. Boult , S. Goldenstein, "Vision of the unseen: current trends and challenges in digital image and video forensics". *ACM Computer Survey*, 2011; 43(4):26:1–26:42.

[2] J. Fridrich, D. Soukal ,J. Lukas, "Detection of copy-move forgery in digital images", *Proc. of digital forensic research workshop, 2003*. p. 55–61.

[3] H. Farid, "Detecting digital forgeries using bispectral analysis", *Technical Report AIM-1657*, AI Lab, Massachusetts Institute of Technology; 1999.

[4] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey", *Digital Investigation*, 2013, *10*(3), 226-245.
http://dx.doi.org/10.1016/j.diin.2013.04.007

[5] Li. Xin, "Blind image quality assessment", *Image Processing. 2002. Proceedings. 2002 International Conference on*. Vol. 1. IEEE, 2002.
http://dx.doi.org/10.1109/icip.2002.1038057

[6] I. Avcibas, S. Bayram ,N. Memon , M. Ramkumar,B. Sankur, "A classifier design for detecting image manipulations", *Proc. International conference on image processing (ICIP)* , 2004. p. 2645–8.

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", *Technical Report TR2004-515*, Department of Computer Science, Dartmouth College; 2004.

[8] D. Fu, Y. Shi, W. Su, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition", *Proc. of International workshop on digital watermarking*, 2006. p. 177–87
http://dx.doi.org/10.1007/11922841_15

[9] S. Bayram , I. Avcibas ,B. Sankur, N. Memon, Image manipulation detection , *Electron Imaging*, 2006;15(4). 041102-1–041102-17
http://dx.doi.org/10.1117/1.2401138

[10] H. Gou, A. Swaminathan, M. Wu, "Noise features for image tampering detection and steganalysis", *Proc. International conference on image processing* (ICIP) 2007. p. 97–100.
http://dx.doi.org/10.1109/icip.2007.4379530

[11] S. J. Ryu, H. Y. Lee, I. W. Cho, & H. K. Lee, " Document forgery detection with SVM classifier and image quality measures", *Advances in Multimedia Information Processing-PCM 2008* (pp. 486-495). Springer Berlin Heidelberg.

[12] Z. Zhang, J. Kang, Y. Ren, "An effective algorithm of image splicing detection", *Proc. International conference on computer science and software engineering*, 2008. p. 1035–9.
http://dx.doi.org/10.1109/csse.2008.1621

[13] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics". *Image and Vision Computing*, 2009, *27*(10), 1497-1503.
http://dx.doi.org/10.1016/j.imavis.2009.02.001

[14] M. Stamm and K. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints", *IEEE Trans Inf Forensics Security*, 2010; 5(3):492–506.
http://dx.doi.org/10.1109/TIFS.2010.2053202

[15] B. Liu and C. M. Pun, "Splicing Forgery Exposure in Digital Image by Detecting Noise Discrepancies", 2015, International *Journal of Computer and Communication Engineering*, *4*(1), 33.
http://dx.doi.org/10.7763/IJCCE.2015.V4.378