International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

A Survey of Fast and Effective Image Forgery Detection Techniques

Neha Sharma* and Pallavi Gupta

Department of Electronic & Communication Engineering, Global Research Institute of Management and Technology, Haryana, India

Received 15 Nov 2022, Accepted 16 Dec 2022, Available online 20 Dec 2022, **Vol.10 (Nov/Dec 2022 issue)**

Abstract

One of the most popular manipulations for altering digital photos is forgery. Due to their resistance to a variety of assaults, including large-scale geometric changes, keypoint-based detection techniques have been claimed to be particularly successful in uncovering copy-move evidence. These techniques, however, fall short in situations when copy-move forgeries only involve tiny or smooth areas, where there are few keypoints. We offer a quick and efficient copy-move forgery detection technique using hierarchical feature point matching to address this issue. We first demonstrate that by reducing the contrast threshold and rescaling the input picture, it is feasible to obtain a significant number of keypoints that exist even in tiny or smooth regions. We then create a brand-new hierarchical matching technique to address.

Keywords: *Forgery, Hierarchical feature, Smooth regions etc.*

Introduction

Unquestionably, the age we live in exposes us to a great variety of visual stimuli. While in the past we might have had faith in the accuracy of these images, this faith is now being eroded by modern digital technologies. Doctored images are becoming more and more prevalent in a variety of contexts, including tabloid publications, the fashion industry, mainstream media, academic journals, political campaigns, courtrooms, and picture hoaxes that show up in our email inboxes. In order to regain some faith in digital photographs, the area of digital forensics has grown during the past five years. I'll go over the current state of the art in this brand-new, fascinating topic.

The idea of using digital watermarking to verify images has been put forth (see, for example, and for general surveys). This method has the disadvantage that a watermark must be added at the time of recording, limiting its use to digital cameras with certain accessories. In contrast to these methods, passive image forensics techniques work without the need of a watermark or signature. These methods operate under the presumption that while digital forgeries would not leave any visible signs of tampering, they might change an image's underlying data. Approximately five categories may be used to classify the collection of picture forensic tools: 1) pixel-based methods for spotting statistical outliers introduced at the pixel level; 2) format-based techniques that take advantage of statistical correlations brought on by a particular lossy compression scheme; 3) camera-based techniques that take advantage of artifacts brought on by the camera lens, sensor, or on-chip post processing; 4) physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that measure objects in the real world.

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr/v.10.6.11

Format Based

In any forensic study, "preserve the evidence" must unquestionably be the first priority. In this sense, lossy picture compression techniques like JPEG may be viewed as the worst possible adversary for forensic analysts. Ironically, forensic analysis can take advantage of the special qualities of lossy compression. I outline three forensic methods for finding evidence of manipulation in compressed pictures, each of which expressly makes use of JPEG's lossy compression strategy.

JPEG Quantization

JPEG is the picture encoding standard used by most cameras. The amount of compression that may be obtained with this lossy compression approach is quite flexible. In order to balance compression and quality according to their individual demands and preferences, manufacturers often setup their products differently. This distinction can be used to determine the source (camera make/model) of an image, as discussed in and.

Following is the normal JPEG compression process for a three-channel RGB colour image: It begins by converting the RGB picture to luminance/chrominance space (YCbCr). In comparison to the luminance channel, the two chrominance channels (CbCr) are commonly subsampled by a factor of two (Y). The next step is to divide each channel into 8 pixel blocks. Unsigned numbers are changed into signed integers for these values (e.g., from). A 2-D discrete cosine transform is used to translate each block into frequency space (DCT). Each DCT coefficient, c, is then quantized by an amount q, which is dependent on the particular frequency and channel:

Double JPEG

Any digital processing at the very least necessitates the loading and resaving of a picture into a photo-editing tool. It is likely that the original and altered photographs are both kept in the JPEG format as this is how most images are saved. The altered picture is compressed twice in this instance. Due to the JPEG picture format's lossy nature, this double compression generates certain artefacts that aren't present in singly compressed images (assuming that the image was not also cropped prior to the second compression). Therefore, the existence of these artefacts can serve as proof of some modification. Keep in mind that using double JPEG compression does not always indicate intentional manipulation.

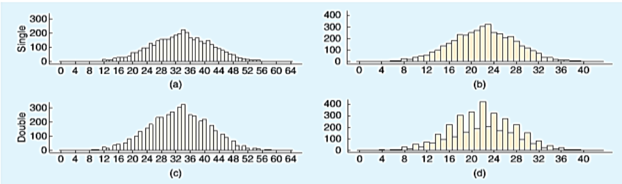

Fig.1 Histograms of single-quantized signals with Steps 2 and 3 are displayed along the top row. Histograms of double-quantized signals are displayed in the bottom row, with (c) Step 3 coming after Step 2, and (d) Step 2 coming after Step 3. Take note of the periodic artefacts in the double-quantized signal histograms.

For example, it is possible to inadvertently save an image after simply viewing it.

As described in the previous section, quantization of the DCT coefficients cis the primary manner in which compression is achieved, denoted as, $q_a(c) = \lfloor c/a \rfloor$,where a is the quantization step (a strictly positive integer). The quantized values are returned to their original range by dequantization: $q_a^{-1}(c) = ac$. It should be noted that dequantization is not the inverse function of quantization and that quantization is not invertible. Double compression leads to double quantization, which is provided by the equation: $q_{ab}(c) = c/b/a$, where a and b are the quantization steps. Three steps can be used to depict the process of double quantization: 1) Quantization with step b, 2) Dequantization with step b, and 3) Quantization with step an are the order of operations. Consider a collection of coefficients that are now evenly spaced out in the range. Take a look at four distinct quantization's of these coefficients to see the nature of the double quantization artifacts. The histograms of the coefficients quantized using steps 2 and 3 are shown in the top row of Figure 1. The histograms of the double-quantized coefficients, with steps 3 followed by 2 and 2 followed by 3, are displayed in the bottom row. Because the first quantization divides the samples of the original signal into 42bins and the second quantization redistributes them into 64bins, certain bins in the histogram are empty as the step size lowers [Figure 1(c)]. Because the even bins acquire data from four initial histogram bins but the odd bins only receive samples from two, certain bins contain more samples than their surrounding bins as the step size grows [Figure 1(d)]. Note the frequency of the artefacts created into the histograms in both instances of double quantization. The authors in their study took use of this periodicity to find double JPEG compression. This method was expanded in order to find specific evidence of double compression.

JPEG Blocking

The block DCT transform serves as the foundation for JPEG compression, as was mentioned in the sections before this one. Since each 8 x 8 pixel picture block is independently converted and quantized, artefacts in the form of horizontal and vertical edges can be seen at the boundary of adjacent blocks. These artefacts may be disrupted during picture manipulation.

Camera Based

Gun barrel grooves give the bullet a spin for better accuracy and range. These grooves provide the fired bullet some recognisable marks, making it possible to associate a bullet with a particular firearm. In

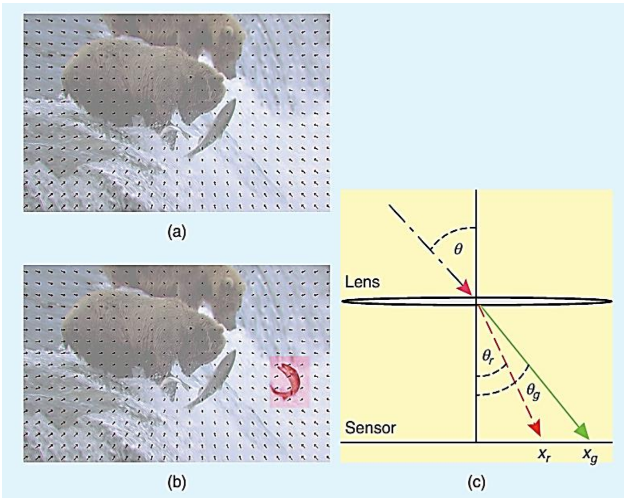

Fig.2 Chromatic aberration: (a) A vector field displaying the pixel displacement between the red and green channels is superimposed on the original picture. (b) The fish was added to this image after being removed from another photograph.

The global pattern is not consistent with its chromatic aberration [FIG2] Chromatic aberration: (a) A vector field displaying the pixel displacement between the red and green channels is superimposed on the original picture. (b) The fish was added to this image after being removed from another photograph. The global pattern is not consistent with its chromatic aberration. In the same vein, a number of picture forensic methods have been created that precisely simulate artifacts added by different imaging process phases. I provide four methods for estimating and modeling various camera artifacts. Then, irregularities in these artifacts can be utilized as proof of manipulation.

Chromatic Aberration

Light enters the imaging system through the lens and is directed to a single spot on the sensor in an ideal imaging system. However, optical systems depart from such ideal models because they are unable to concentrate light of all wavelengths properly. Laminar chromatic aberration specifically shows itself as a change in the areas where light of various wavelengths enters the sensor. The authors of demonstrate in that the expansion or contraction of the colour channels with regard to one another can approach this lateral aberration. An illustration of a picture with a vector field overlaid on it to indicate the red channel's misalignment with the green channel is shown in Figure 2(a). This identical image with the fish added to it is seen in Figure 2(b). The local lateral aberration in this modified location is in conflict with the overall aberration, as you can see. In order to identify this kind of manipulation, the authors of explain how to calculate lateral chromatic aberration.

Color Filter Array

Three channels, such as red, green, and blue, each include samples from a distinct band of the colour spectrum, make up a digital colour picture. However, the majority of digital cameras only use a single CCD or CMOS sensor and use a colour filter array to create colour pictures (CFA). The majority of CFAs use red, green, and blue colour filters on top of each sensor element. The other two colour samples must be inferred from the nearby samples in order to create a three-channel colour picture because only one colour sample is captured at each pixel position. CFA interpolation or demosaicking is the process of estimating the missing colour samples. Kernel-based demosaicking techniques that act on each channel separately are the most basic (e.g., bilinear or bicubic interpolation). In order to prevent blurring important visual details, more advanced algorithms interpolate edges differently from uniform regions. CFA interpolation introduces particular statistical correlations between a group of pixels in each colour channel, regardless of the implementation.

Literature Survey

Hu, Wu-Chih et al. (2016) [1] Using picture watermarking and alpha mattes, this research presents an efficient method for detecting altered foreground or background images. The foreground and background pictures are generated using the suggested method's component-hue-difference-based spectral matting, which is based on the alpha matte. Then, two separate watermarks are embedded into the foreground and background pictures, respectively, using image watermarking based on the discrete wavelet transform, discrete cosine transform, and singular value decomposition. The difference between the singular values acquired is then utilised to determine if the foreground or background picture has been altered. The suggested technique performs effectively in terms of picture forgery detection, according to experimental data.

Chauhan, Devanshi, et al. (2016) [2] One of the issues in image forensics discussed in this study is determining a picture's validity. When photographs are used as proof that alters judgement, such as, for instance, in a court of law, this may be a highly significant duty. While there are several ways to fake an image, copy-move forgery is the most popular. Copy-move forgeries are made by copying a section from one image and putting it on another to deceive the user. This kind of forgery is carried out utilising modern, sophisticated software and programmes that are readily available. Video forgeries of this nature are also practised. We review many keypoint-based copy-move forgery detection techniques with various parameters in this research.

Chierchia, Giovanni 2014 [3] The most recent generation of graphics editing applications offer ever-more-powerful capabilities that enable the retouching of digital photos with little to no evidence of manipulation. Therefore, a variety of complementing technologies that take use of various picture features are needed for the effective identification of image forgeries. The most useful of these tools are methods based on the photo-response non-uniformity (PRNU) noise because they don't look for the inserted object but rather the absence of the camera's PRNU, which functions as a kind of camera fingerprint and effectively detects forgeries that most other methods miss. In this study, we provide a fresh method for identifying faked images by analysing sensor pattern noise.

Hu, Wu-Chih, 2016 [4] This study suggests a useful method for detecting altered foreground or background images utilising image watermarking and alpha mattes. The foreground and background pictures are generated using the suggested method's component-hue-difference-based spectral matting, which is based on the alpha matte. Then, two separate watermarks are embedded into the foreground and background pictures, respectively, using image watermarking based on the discrete wavelet transform, discrete cosine transform, and singular value decomposition. The difference between the singular values acquired is then utilised to determine if the foreground or background picture has been altered. The suggested technique performs effectively in terms of picture forgery detection, according to experimental data.

Muhammad, Ghulam 2014 [5] This study proposes a new technique for detecting fake images using the steerable pyramid transform (SPT) and local binary pattern (LBP). A colour picture is first transformed in the YCbCr colour space, and the chrominance channels Cb and Cr are then subjected to the SPT transform, resulting in a variety of multi-scale and multi-oriented subbands. Then, we use LBP histograms to characterise the texture in each SPT subband. A feature vector is created by concatenating the histograms from each subband. The feature vector is then used by a support vector machine to categorise pictures as being fake or real. Three publicly accessible picture datasets have been used to assess the suggested technique. The usefulness of the suggested approach and its superiority to certain more current methods are shown by our experimental results.

Pun, Chi-Man, Xiao-Chen 2015 [6] This work proposes an innovative feature point matching and adaptive oversegmentation copy-move forgery detection method. The suggested solution incorporates keypoint-based and block-based forgery detection techniques. The host picture is first adaptively segmented into nonoverlapping and irregular chunks by the suggested adaptive oversegmentation technique. The labelled feature points are then located by extracting the feature points from each block as block features and matching them with one another; this technique might roughly identify the suspected forging locations. We suggest the forgery area extraction approach, which creates merged regions by merging surrounding blocks with comparable local colour characteristics into the feature blocks in place of the feature points in order to more correctly detect forgery regions.

Ansari, Mohd 2014 [7] A digital image may be readily edited thanks to the development of digital image processing software. Because a picture may be used as evidence in court, forensic investigations, and many other sectors, the identification of image modification is crucial. The goal of pixel-based picture forgery detection is to confirm the veracity of digital images without having access to the source image beforehand. There are several techniques to alter a picture, including splicing or copy-moving, resampling (resize, rotate, stretch), adding or removing any item from the image, and many more. The major copy-move and splicing strategies for pixel-based picture forgery detection have been covered in this work.

Rad, Reza Moradi 2015 [8] The validity of digital photos has been questioned by the introduction of sophisticated yet user-friendly modification programmes. Therefore, it is crucial to create trustworthy detection methods in order to confirm an image's uniqueness. In this study, a forgery detection method based on edge information analysis is suggested. Contrary to standard approaches, the suggested methodology permits the input picture to be singly compressed or uncompressed rather than being limited to the traces left by the act of double compression. The suggested approach may localise forged region when the forged picture is not double compressed, according to experimental results.

Qazi, Tanzeela 2013 [9] The determination of the authenticity of multimedia information has become a difficult problem as a result of the mushroom proliferation of cutting-edge digital picture and video editing technologies. Digital image forensics is a rapidly expanding scientific subject that represents the never-ending fight against fraud and manipulation. This survey aims to cover the blind methods for forgery detection that have been suggested. This study focuses on three of the most popular forgery types—copy/move, splicing, and retouching—and the detection methods for each.

Qureshi, M. Ali, and M. Deriche 2014 [10] The ability to manipulate photographs and change their content is now commonplace thanks to the development of robust image editing software. Important aspects may now be added, changed, or removed from an image without leaving any perceptible signs of manipulation. It is critical to create reliable detection systems to spot image tampering activities given the daily upload of more than several million images to the internet and the advent of e-Government services. By revealing manipulation tactics, picture forensics tools seek to reestablish confidence and acceptability in digital media. This study focuses on such detection strategies. With a focus on copy and move methods, we give an overview of several forging detection techniques.

Huynh, Tu K.,2015 [11] A overview of Image Forgery Detection (IFD) methods used for Copy-Move and spliced pictures is presented in this research. The survey aims to categorise engaged algorithms into groups with comparable approaches to problem-solving during the last 10 years. When classifying Copy-Move pictures, the distinction between processing input images with or without modification before extracting image characteristics must be taken into account. Groups of detecting methods based on camera characteristics or image features are summarised for the spliced pictures. As guides and resources for the upcoming studies, this book also mentions the approaches' successes, drawbacks, and upcoming endeavours.

Isaac, Meera Mary 2015 [12] Due to the rising amount of fake photos being shared on the Internet and other social media, as well as the legal and societal problems they are causing, the detection of image forgery has become a hot topic in study. The researchers' main challenge is determining if a picture is fake or real and locating the fraud. Numerous approaches were put forth, but no effective technique that can reliably identify picture counterfeiting has yet been developed. Here, we provide a cutting-edge method for identifying fake images that uses the texture of the original picture as a differentiating characteristic. The technique uses Local

Phase Quantization (LPQ), which may extract pertinent texture characteristics and provide them as input to a Support Vector Machine for classification. Gabor wavelets are also used in the technique. The results show that the DVMM colour dataset and CASIA v1 both have accuracy levels of > 99%. It performs better than other cutting-edge techniques for detecting picture counterfeiting.

Sunil, Kumar 2014 [13] One of the most popular study topics in the field of picture forensics is the identification of copy move forgeries. Numerous methods have been proposed to identify this kind of tampering with the original image, however many problems are still open or have room for improvement. Block matching method is the most often used approach to find this kind of manipulation. The time required by the detection approaches and robustness against post-processing activities are a couple of the main obstacles. One post-processing action the attacker may use to get around picture forgery detection techniques is changing the intensity of the copied region. The suggested method successfully addresses this. The feature vector of overlapping blocks has been represented and compressed using discrete cosine transform and principal component analysis, respectively. Utilizing down sampling of low frequency DCT coefficients, features are produced that are insensitive to local changes in intensity.

Chauhan, Devanshi 2016 [14] Verifying a picture's validity is one of the issues with image forensics. When photographs are used as proof that alters judgement, such as, for instance, in a court of law, this may be a highly significant duty. While there are several ways to fake an image, copy-move forgery is the most popular. Copy-move forgeries are made by copying a section from one image and putting it on another to deceive the user. This kind of forgery is carried out utilising modern, sophisticated software and programmes that are readily available. Video forgeries of this nature are also practised. We review many keypoint-based copy-move forgery detection techniques with various parameters in this research.

Proposed Work

Digital material may now be changed and used in ways that were just not feasible twenty years ago thanks to technology. The technology of the future will almost likely enable us to modify digital material in ways that are currently unthinkable. It will also be more crucial than ever for the science of digital forensics to try to stay up with this technology as it develops.

There is no doubt that new ways will be developed to produce better fakes that are more difficult to identify as we continue to improve tools for uncovering photographic frauds. While certain forensic technologies could be simpler to trick than others, most users won't be able to get around some of them. By simply putting a picture into its original lattice and reinterpolating each colour channel, one may, for instance, restore the colour filter array interpolation after it has been disrupted. On the other hand, a typical photo-editing application makes it difficult to adjust for erratic lighting. An arms race between the forger and the forensic analyst is partly inevitable, much like in the virus/antivirus and spam/antispam games. However, the study of picture forensics has made it more difficult and time-consuming (but never impossible) to produce a fake that cannot be found.

Objectives

1. To Study and analyze various image forgery techniques.
2. To Propose a new DCT based method for forgery identification
3. To implement and evaluate the proposed scheme using various metrics such as MSE, detection probability etc.

Conclusion and Future Scope

The method for estimating a quantization step from a given picture is proposed in this paper. The work proposes a quantization fingerprint—the number of integer quantized forward coefficients—by analysing the quantization effect during the JPEG compression and decompression pipeline. It also provides a mathematical justification to demonstrate the relationship between local maxima of that measure and the actual quantization step. Based on the quantization fingerprint and the statistical model of DCT coefficients presented in our earlier research, the estimate technique was created. Numerical tests on a sizable picture database demonstrate the applicability of the suggested strategy. The high estimation accuracy for a wide range of photos with various image contents, image sizes, and quality parameters is the suggested method's main strength. Additionally, although some previous approaches fail, the suggested method can accurately estimate the quantization steps for DC coefficients. Applying the suggested approach to actual colour JPEG photographs obtained from various camera models/brands emphasises how accurate it is. The resilience of the proposed approach against colour noise created during the JPEG compression process is demonstrated by the good performance on colour pictures. The suggested technique takes longer than existing ones while having higher estimation accuracy performance. This flaw results from the use of a numerical optimization approach for ML estimate of the DCT model parameters. The suggested approach also demonstrates its accuracy in additional real-world forensic situations, such as the estimate of the secondary quantization table in a double-JPEG compressed picture stored in lossless format and the detection of JPEG compression. This strategy could be investigated in more forensic circumstances in the future. By examining the properties of double-JPEG compression and determining the relevant version of the IQF fingerprint, this technique may be extended for the detection of double-JPEG compression existence and estimate of the principal quantization table in a double-JPEG compressed picture. Due to the strong efficiency of the suggested approach for JPEG compression identification on small-size pictures, the second forensic application uses discrepancies in JPEG compression history among various regions of the image under examination to identify and pinpoint copy-paste forgeries. As various manufacturers create their own compression schemes, picture origin identification is another forensic application that seeks to confirm if the image in issue was captured by a certain source (camera equipment, model, brand).

References

[1] Chierchia, Giovanni, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. "A Bayesian-MRF approach for PRNU-based image forgery detection." IEEE Transactions on Information Forensics and Security 9, no. 4 (2014): 554-567.

[2] Jaberi, Maryam, George Bebis, Muhammad Hussain, and Ghulam Muhammad. "Accurate and robust localization of duplicated region in copy–move image forgery." Machine vision and applications 25, no. 2 (2014): 451-475.

[3] Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi. "Pixel-based image forgery detection: A review." IETE journal of education 55, no. 1 (2014): 40-46.

[4] Sunil, Kumar, Desai Jagan, and Mukherjee Shaktidev. "DCT-PCA based method for copy-move forgery detection." In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II, pp. 577-583. Springer International Publishing, 2014.

[5] Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive oversegmentation and feature point matching." IEEE Transactions on Information Forensics and Security 10, no. 8 (2015): 1705-1716.

[6] Huynh, Tu K., Khoa V. Huynh, Thuong Le-Tien, and Sy C. Nguyen. "A survey on image forgery detection techniques." In Computing & Communication Technologies-Research, Innovation, and Vision for the Future (RIVF), 2015 IEEE RIVF International Conference on, pp. 71-76. IEEE, 2015.

[7] Isaac, Meera Mary, and M. Wilscy. "Image forgery detection based on Gabor Wavelets and Local Phase Quantization." Procedia Computer Science 58 (2015): 76-83.

[8] Rad, Reza Moradi, and KokSheik Wong. "Digital image forgery detection by edge analysis." In Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on, pp. 19-20. IEEE, 2015.

[9] Hu, Wu-Chih, Wei-Hao Chen, Deng-Yuan Huang, and Ching-Yu Yang. "Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes." Multimedia Tools and Applications 75, no. 6 (2016): 3495-3516.

[10] Chauhan, Devanshi, Dipali Kasat, Sanjeev Jain, and Vilas Thakare. "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image." Procedia Computer Science 85 (2016): 206-212.

[11] Chierchia, Giovanni, et al. "A Bayesian-MRF approach for PRNU-based image forgery detection." IEEE Transactions on Information Forensics and Security 9.4 (2014): 554-567.

[12] Hu, Wu-Chih, et al. "Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes." Multimedia Tools and Applications 75.6 (2016): 3495-3516.

[13] Muhammad, Ghulam, et al. "Image forgery detection using steerable pyramid transform and local binary pattern." Machine Vision and Applications 25.4 (2014): 985-995.

[14] Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive oversegmentation and feature point matching." IEEE Transactions on Information Forensics and Security 10.8 (2015): 1705-1716.

[15] Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi. "Pixel-based image forgery detection: A review." IETE journal of education 55.1 (2014): 40-46.

[16] Rad, Reza Moradi, and KokSheik Wong. "Digital image forgery detection by edge analysis." Consumer Electronics-Taiwan (ICCE-TW), 2015 IEEE International Conference on. IEEE, 2015.

[17] Qazi, Tanzeela, et al. "Survey on blind image forgery detection." IET Image Processing 7.7 (2013): 660-670.

[18] Qureshi, M. Ali, and M. Deriche. "A review on copy move image forgery detection techniques." Systems, Signals & Devices (SSD), 2014 11th International Multi-Conference on. IEEE, 2014.

[19] Huynh, Tu K., et al. "A survey on image forgery detection techniques." Computing & Communication Technologies-Research, Innovation, and Vision for the Future (RIVF), 2015 IEEE RIVF International Conference on. IEEE, 2015.

[20] Isaac, Meera Mary, and M. Wilscy. "Image forgery detection based on Gabor Wavelets and Local Phase Quantization." Procedia Computer Science 58 (2015): 76-83.

[21] Sunil, Kumar, Desai Jagan, and Mukherjee Shaktidev. "DCT-PCA based method for copy-move forgery detection." ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing, 2014.