AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/AEB/

A Review of Image Forensics

[1]Shokouh Neshat Safavi and [2]Hossein Malekinezhad

[1]*Mahallat branch, Islamic Azad University, Mahallat, Iran.*
[2]*Naragh branch, Islamic Azad University, Naragh, Iran.*

ARTICLE INFO

Article history:
Received 15 April 2014
Received in revised form 22 May 2014
Accepted 25 May 2014
Available online 15 June 2014

Keywords:
Forensic, Image authentication, Acquisition, Image coding, Image editing

ABSTRACT

The aim of this survey is to provide a comprehensive overview in the area of image forensics. These techniques have been designed to identify the source of a digital image or to determine image authentication, without the knowledge of any prior information about the image under analysis. All of the proposed methods is based on imaging devices and doing processes that the presence or absence of incongruence reveal in normal mode of picture. This paper has been organized into three categories by classifying the tools according to the position in the history of the digital image: acquisition-based methods, coding-based methods and editing-based methods.

To Cite This Article: Shokouh Neshat Safavi and Hossein Malekinezhad., A Review of Image Forensics. ***Adv. Environ. Biol., 8(11),*** *1417-1424, 2014*

INTRODUCTION

Image unlike text, is an effective communication medium that it is possible to understand its content simply. Always images were used to validate the news in the past. Now, with the advances of digital technology and image editing tools, less experienced people can easily modify the content of images and create fake images. Hence Pictures, no longer are not reliable [1-3]. With these conditions, are needed to methods that be evaluated through they experience and credibility a digital image. These methods are shown in Figure 1 are divided into two groups: active methods and passive methods.

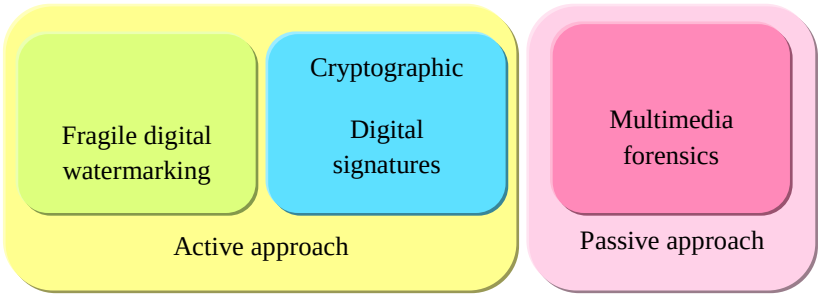

Fig. 1: A variety assessment methods of the history and credibility of a digital image.

In active method, to assess the reliability, some of data in the source are calculated during imaging are being exploited, while in passive method is just trying to be evaluated a digital image content. In active method by using a trustworthy camera, a digital watermark or a digital signature at the instant of acquisition is reviewed and are detected any changes in the image [4-6].

A major drawback of this method is that digital cameras are equipped with a watermarking chip or a digital signature chip and using the private key embedded in the camera, authenticates every image that recorded by the camera before storing on memory card. In passive method, are detected multimedia forensics based on observation that at any stage of the process leaves a distinctive trace on the data as a sort of a digital signature [7,8].

Thus image authentication by detecting the presence or absence of some indication in the content of the image is possible. The task of multimedia forensic tools is to expose the traces left in multimedia content by

Corresponding Author: Shokouh Neshat Safavi, Mahallat branch, Islamic Azad University, Mahallat, Iran.
E-mail: shneshat7@gmail.com

exploiting existing knowledge in digital image. The research activity in this domain started a few years ago and increased in the last months, therefore, we have provided an overview of the forensic methods in digital images. The paper is organized as follows: section 2 presents the steps of the life cycle from a digital image. In section 3 the effects of image acquisition is described. In section 4 Coding-based methods are briefly explained and section 5 describing editing-based methods. Finally, the results of the research in this domain and the work that we intend to accomplish in the future, are drawn in section 6.

2. Digital Image Life Cycle:

As indicated in figure 2, the life cycle of a digital image is composed of three main steps: acquisition, coding and editing.

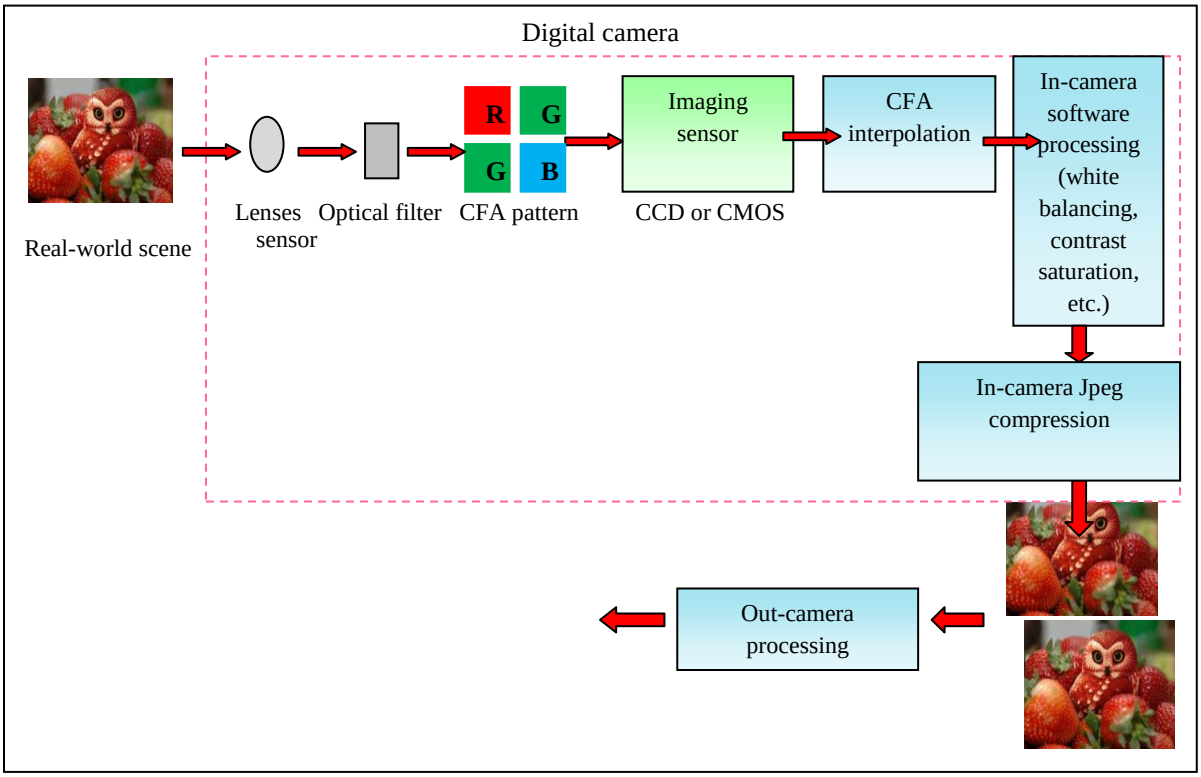

Fig. 2: Construction stages of the lifecycle of a digital image.

During acquisition, the lenses on the camera sensor focus the light coming from the real scene framed by the digital camera, where the digital image signal is generated. Before reaching the sensor, the light is usually filtered by the CFA that permits a certain component of light to pass through it to the sensor. To each pixel, only one particular main color (Red, Green or Blue) is gathered. The sensor output is interpolated through the so-called demosaicing process to obtain these three main colors for each pixel and in order to obtain the digital color image. With coding, the processed signal is stored on the camera memory (usually for storage, of lossy compression is used). Finally, the generated image can be post processed to enhance or to modify content. During the life of an image any image editing such as rotation, blurring, contrast adjustment and etc may be applied to it. Finally, after editing, often the image is saved in JPEG format and recompression will occur. The idea of image forensics is that the effects of any image processing at its history are left. These effects can be extracted and analyzed for understanding the history of digital content. According to the image life cycle, we will describe below acquisition fingerprints, coding fingerprints and editing fingerprints.

Acquisition fingerprints: Each component in a digital acquisition device modifies the input and leaves intrinsic fingerprints in the final image output, due to the specific optical system, image sensor and camera software. In each step, camera introduces imperfections or intrinsic image regularities that these effects remain in the final image.

Coding fingerprints: Lossy compression leaves itself characteristics footprints, which are related to the specific coding architecture.

Editing fingerprints: Each processing applied to the digital image, even if not visually detectable, modifies properties of the image.

Then the previous traces can be used to source identification and tampering detection. In the case of source identification, some acquisition traces are usually extracted from the image under analysis, and then compared

with a dataset of possible fingerprints specific for each class/ brand/ model of device. The most similar fingerprint in the dataset indicates the device that looks the image. In the case of forgery detection, the aim to expose traces of semantic manipulation, according to two possible strategies: detecting inconsistencies or the absence of acquisition and coding fingerprints within the considered image indirectly reveals that some post processing destroyed them, detecting the presence of editing fingerprints representing a given post processing directly reveals the manipulation.

3. Acquisition-Based Methods:

In this section traces left in image by the lens, the sensor and the color filter array will be checked.

Effects caused by lens:

Each acquisition device model presents individual lens characteristics. Lenses leave unique traces on the images being captured that can be used to link an image to a particular device or to discover the presence of image modifications. Lenses due to design and manufacturing process produce several types of deviations. For example in lateral chromatic aberration, lens aberration caused different light wavelengths to focus on shifted points in the image represented by the sensor. When the source light is off the optical axis, resulting in a misalignment between color channels, as shown in Figure 3. By assuming that the lateral chromatic aberration is constant within each of t5he three color channels and by using the green channel as a reference, the aberrations between the red and green channels and between the blue and green channels are estimated.

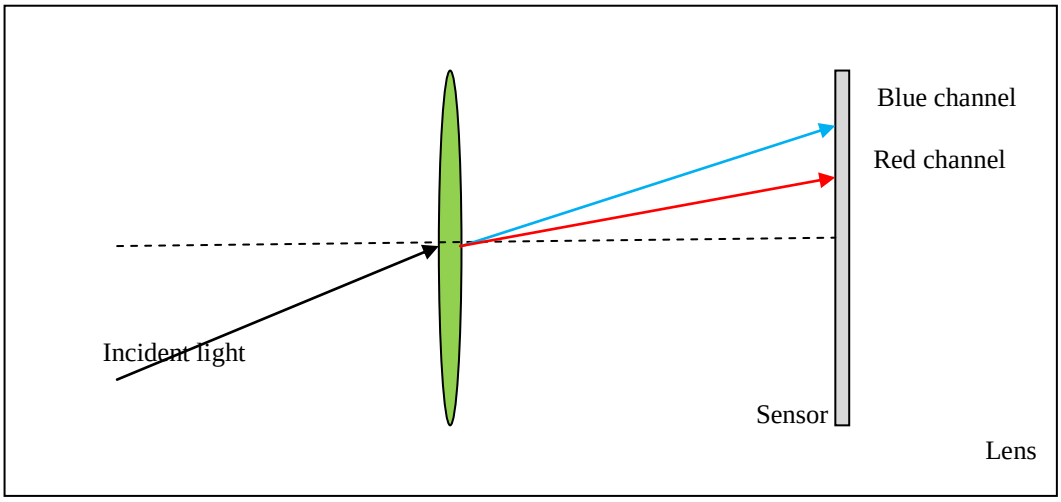

Fig. 3: A sketch of the lateral chromatic aberration.

Johnson *et al*., [9] detect image forgeries by looking for the presence of local deviations or inconsistencies in low-parameter model (with respect to the parameters obtained for the whole image). Existence inconsistency is means that the image is manipulated [9]. The method proposed by Yerushalmy *et al*., [10] is based on PFA (in form of a blue purple halo near the edges of objects in the image), that although having a much more complex origin, is stronger and more visible than lateral chromatic aberration. In this method from inconsistencies in PFA are used for tampering detection [10].

Effects caused by sensor:

Sensor pattern noise, due to imperfections of the image sensor, resulting in slight differences between the sensed scene and the image acquired by the camera. Janesick, [11] reported during the research that the dominating component of sensor pattern noise is PRNU noise that due to a combination of factors including imperfections during the CCD/CMOS manufacturing process, silicone in-homogeneities and thermal noise. The overall PRNU is a high frequency multiplicative noise that is stable throughout the camera's lifetime in normal operating conditions and is unique to each camera. These properties make PRNU adapt for device identification, for single device linking and if inconsistencies in the PRNU pattern within the image are found in certain regions, for tampering detection [11]. Most of the successive works in this area focuses on making the PRNU estimation more robust. Liu *et al*., [12] reported in the research that the PRNU is estimated based on regions of high SNR between estimated PRNU and total noise residual to minimize the impact of high frequency image regions [12]. Li, [13] propose a scheme attenuates strong PRNU components, which are likely to have been affected by high frequency image components [13].

Effects caused by CFA:

Along with PRNU, another important effect left by camera during acquisition is that due to the presence of the color filter array. Indeed, excluding professional CCD/ CMOS cameras, the incoming light is filtered by the color filter array before reaching the sensor, as shown in figure 4, so that for each pixel only one particular color is gathered.

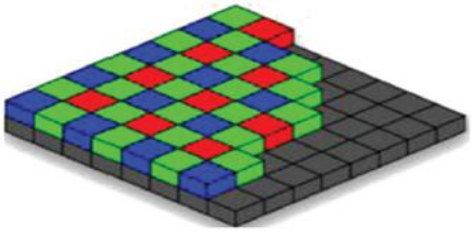

Fig. 4: An example of color filter array [14].

To obtain the missing pixel values for the three-color layers is used demosaicing process. This process leaves specific correlations in the image pixels that are detectable. Ideally an image coming from a digital camera, in the absence of any successive processing, will show demosaicing effects; on the contrary, demosaicing inconsistencies between different parts of the image, as well as their absence in all or part of the analyzed image, will put image integrity in doubt. Popescu *et al*., [15] proposed a technique for detecting the presence of CFA interpolation in an image by assuming linear interpolation kernel, this simplistic hypothesis compared to complex methods adopted in commercial devices and using an EM algorithm to estimate its parameters and the pattern of the filter. This method determine a *p*-map, which identifies for each pixel the probability of being correlated to neighboring pixels. Analysis this correlation map exhibit a periodic behavior which is clearly visible in the Fourier domain and it is used to tampering detection in image [15].

4. Image Coding-Based Methods:

Lossy image compression is one of the most common operations, which is performed on digital images, because it is easier to store or transport smaller amounts of data. Indeed, most digital cameras compress each image after taking a shot. Respect to lossy compression nature, image coding leaves characteristic footprints that are detectable. By exposing the effects of coding in digital images, image forgery is determined. In general, the following methods are used to detect compression in the images:

Standard JPEG:

Nowadays, JPEG is the most common compression standard. This type of compression is consists of three steps: DCT , Quantization and Entropy coding [16].

Algorithms for the identification of compression history:

To know the image history, in particular to detect whether that image had been previously compressed and to determine the compression parameters, the algorithms are used that can be revealed evidences of residual compression in the pixel domain or in the transform domain. In case of residual effects in the pixel domain, Fan et al., 2003 propose a method capable of revealing compression effects also when very light JPEG compression is applied. In this method quality factor Q is high 95. The proposed algorithm is based on the idea that if the image has not been compressed, the pixel differences across 8*8 block boundaries should be similar to those within blocks. Then, it is possible to build two functions Z' and Z", taking into account inter and intra block pixel differences. The energy of the difference between the histograms of Z' and Z" is compared to a threshold and if it is higher that this threshold, the presence of prior compression is deduced 1[7]. In case of residual effects in the transform domain, Lou *et al*., [18] propose a method based on the observation that in a JPEG compressed image, the integral of the DCT coefficient histogram in the r4ange (-1, +1) is greater than the integral in the range (-2, -1] ∪ [+1, +2), with quantization steps that are equal to or larger than 2. By examining the ratio between the first and the second integral, it is possible to verify that its value, in case of JPEG compressed image will be close to zero and this image would be much smaller than that of the corresponding uncompressed one. So, JPEG compression is detected when the ratio is smaller than a given threshold [18].

Algorithms for the estimation of quantization step:

If the image under analysis has been detected as being previously compressed using JPEG, the next problem is to estimate the compression parameters used. In the case of JPEG, this problem means estimating the used quality factor Q or the quantization matrix $\Delta(i, j)$, $1 \leq i, j \leq 8$. Ye et al., 2007 propose a method for estimating the elements of the whole quantization table. To this end, separate histograms are computed for each DCT coefficient sub band. Analyzing the periodicity of the power spectrum of the histogram, it is possible to

extract the quantization step Δ(i, j) for each sub band. Periodicity is detected with a method based on the second-order derivative applied to the histograms. Moreover, blocking effect inconsistencies may tell the presence of tampering [19].

Double JPEG:

The JPEG format is adopted in most of the digital cameras and image processing tools. Thus, we can expect that a manipulated content will often be a recompressed JPEG image. Thus, the presence of tampering can be detected by analyzing proper effects introduced by JPEG recompression when the forged image is created. These effects can be categorized into two classes: A-DJPG uses a discrete cosine transform grid aligned and NA-DJPG uses a discrete cosine transform grid nonaligned. Figures 5 and 6 show this two types of compression.

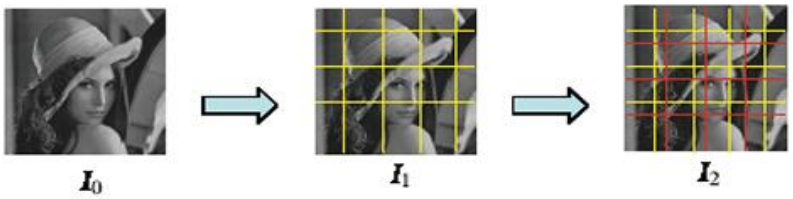

Fig. 5: An example of nonaligned double JPEG compression: the uncompressed image I_0 is first compressed, with a block grid shown in yellow, obtaining a single compressed image I_1; this image is again compressed, with a block grid shown in red, misaligned with the previous one, obtaining the final image I_2 [12].

Fig. 6: An example of aligned double JPEG compression: the uncompressed image I_0 is first compressed, with a block grid shown in yellow, obtaining a single compressed image I_1; this image is again compressed, with a block grid shown in red, aligned with the previous one, obtaining the final image I_2 [12].

Lukas et al., 2003 proposed a scheme to detect the presence of A-DJPG by observing that consecutive quantization introduce periodic effects into the histogram of DCT coefficients. These periodic effects are visible in the Fourier domain as strong peaks in medium and high frequencies and are defined as double quantization (DQ) effects. These peaks in the histogram assume different configurations according to the relationship between the quantization steps of the first group and of the second group compressions. Special attention is paid to the presence of the double peaks and missing centroids in the DCT coefficient histograms, these points are said to be robust features and provide information about the primary quantization [20].

Ou et al., 2008 is proposed a method that covering the NA-DJPG case. In this research by assuming that the image signal is the result of the superposition of different components that are mixed together in the resulting image, ICA is adopted to identify the different contributions and separate them into independent signals. Tampering identification is still performed by means of a classifier. Results are improved 5% , when tampered regions are small [21].

5. Image Editing-Based Methods:

By image editing, any processing applied to the digital media. Change an image may be done for different reasons such as improving its quality or modify its semantic content. Refer to the first edition as innocent editing in which the processed image will carry the same information as the original image but in a more usable and pleasant way. Refer to the second edition as malicious editing in which the semantic information conveyed by the image is changed (usually by adding or hiding one object). Figure 7 demonstrates a simple classification of three categories of editing operators along with examples for each category.

The most important malicious modifications are the copy-move attacks and cut-and-paste attacks. Of course the cut-and-paste attack is more common than the copy-move attack for more flexibility and allows the creation of images with a very different content with respect to the original image. Generally, two methods are used to detect editing on images: signal processing-based techniques and geometry/ physics-based techniques.

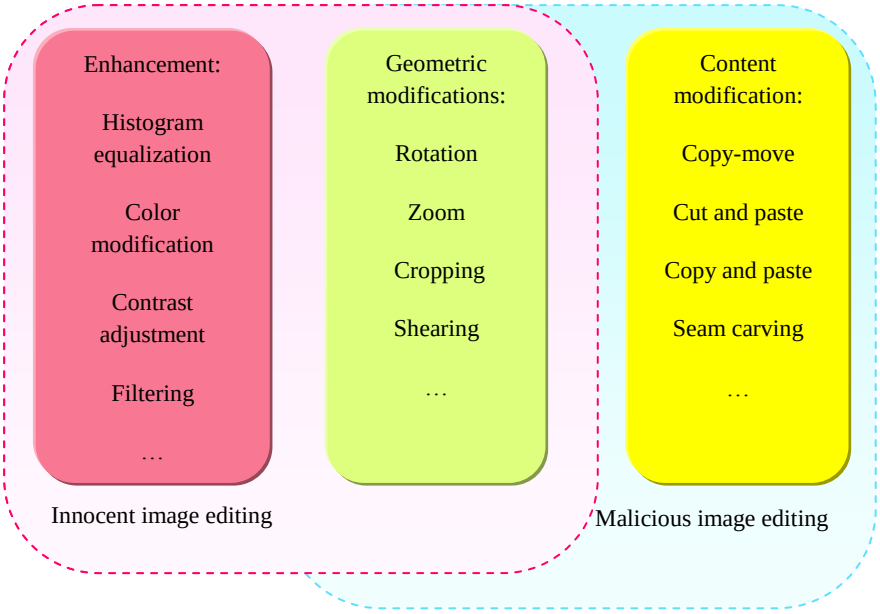

Fig. 7: Types of editing operators applicable to images.

Signal processing-based techniques:

These methods designed to reveal footprints left during the editing stage. For this purpose, the following methods are used:

Copy-Move detection:

This attack consists in copying a portion of an image (of arbitrary size and shape) and pasting it in another location of the same image. Clearly, this technique is useful when the forger wants to hide or duplicate something that is already present in the original image. A block matching procedure was presented by Fridrich *et al*., [22] which inspired the development of several other works in this direction. According to the proposal, instead of looking for the whole duplicated region, the image is segmented into overlapping square blocks and then similar connected image blocks are looked for. By assuming that the cloned region is bigger that the block size, then this region is composed by many overlapping cloned blocks, each cloned block will be moved with the same shift, and thus the distance between each duplicated block pair will be the same. Therefore, the forgery detection will look for a minimum number of similar image blocks within the same and connected to each other to form to image areas exhibiting same shape [22].

Resampling detection technique:

Users often apply to an image geometric transformations like a resizing and/ or rotation. These operators apply in the pixel domain and affecting the position of samples so the original image must be resampled to a new sampling lattice. Resampling leaves specific correlations in the image that can be used as an evidence of editing. These techniques can be detected both benign editing (e.g. scaling or rotation of the whole image) as well as malicious editing. Mahdian *et al*., [23] has been developed a method to resampling detection that studied the periodic properties of the covariance structure of interpolated signals and their derivatives. The core of the proposed scheme is a Radon transform applied to the derivative of the investigated signal, followed by a search for periodicity [23].

Enhancement detection:

Today, it is becoming more and more difficult to find images, which are published without having undergone at least some enhancement operation like smoothing, contrast enhancement, histogram equalization and median filtering. Yuan, [24] proposed an algorithm for the detection of median filtering. Important results of this research is that the two dimensional median filter significantly affects the order or the quantity of the gray leaves in the image area encompassed by the filter window [24].

Seam carving detection:

The basic idea of seam carving is to automatically detect, if any paths of pixels (seams) of the image along which no relevant content is present. Sarkar *et al*., [25] proposed a method which changes in pixel values near

the removed seams are searched by building a Markov model for the co-occurrence matrix in the pixel and frequency domain and used as features to train a classifier [25].

General intrinsic footprints:

This method looks for general footprints left in the signal and detects many tampering with lower accuracy. According to this method a manipulation like splicing bring anomalies in the image statistics, which make them distinguishable from the original images. Respect to this idea that a splicing operation may introduce a number of sharp transitions such as lines, edges and corners, Chen *et al*., [26] employ a classifier that fed with three categories of features highlighting the presence of such traces: statistical moments of the characteristic function (CF) of the image, moments of the wavelet transform of the CF and low-order statics of the 2D-phase congruency. Accuracy, computed over a well-known splicing dataset (the Columbia image splicing detection evaluation dataset), is on the average still below 85% [26].

Geometry/ physics-based techniques:

These techniques reveal inconsistencies introduced at the scene level (e.g. inconsistencies in lighting, shadows, colors, perspective, etc). This method is extremely robust to compression, filtering and other image processing operations. Since in this technique, it is really difficult to create forgery that is consistent from a geometric/ physic point of view, most forgeries contain slight errors, that whether not visible to the human eye, but can be detected by applying proper analysis.

Splicing detection based on lighting/ shadows:

To cutting an object from a photo and pasting it into another photo, requires to adapt object illumination and to introduce consistent shadows in the scene. When this is not done, inconsistencies in lighting direction and shadows can reveal that the forged image is not real. Johnson *et al*., [27] in the research consider the presence of multiple diffuse lighting sources or directional lighting. In this research is estimated the lighting environment some simplifying hypothesis means infinitely distant light sources, lambertian surfaces and etc, under which a nine dimensional model is sufficient to describe mathematically the illumination of the scene. Inconsistencies in the lighting model across in image are used as evidence of tampering [27].

Splicing detection based on inconsistencies in geometry/ perspective:

Since the human brain is not good at evaluating the geometrical consistency of a scene, some works have been developed to detect the presence of inconsistencies in the geometrical and perspective setting of the scene in an image. When the image manipulation involves adding or changing of text, it is usually easy to obtain a convincing fake image. Interesting approach has been proposed by Kakar *et al*., [28] this method is based on inconsistencies in motion blur in the image and usually caused by the slow speed of the camera shutter relative to the object being imaged. The proposed algorithm resorts to a blur estimation through spectral characteristics of image gradients and can detect inconsistencies in motion blur [28].

6. Conclusion and Future Works:

In this paper, the possible methods categorized for detecting forensics in images and briefly discussed. Efficiency and success rate of detecting forged images using acquisition-based methods is higher than other two methods. The main problem in these methods is that the images should be recorded under controlled conditions; also many images must be available for a single device that it is not always possible. Using coding based methods is detected JPEG compression applied to the image, in addition are also identified the effects of compression and quantization parameters used. Using editing based methods are identified effects caused by editing operations in the signal level and in the scene level. In this method a forge is invisible of sight the scene level, is detectable by using work' tools in the signal level and vice versa. In addition work' tools in the signal level can be detect a non-malicious process such as enhances the contrast that is outside of afford work' tools in the scene level. However, work' tools in the scene level are more resistant than work' tools in the signal level against improvement or compression.

In future research, we intend to create a method that without need to the operator with the highest accuracy and the lowest error, can be detect any malicious change in the image.

REFERENCES

[1] Meyer, G.W., H.E. Rushmeier, M.F. Cohen, D.P. Greenberg, K.E. Torrance, 1986. An experimental evaluation of computer graphics imagery. ACM Transactions on Graphics, 5: 30-50.
[2] Farid, H., 2006. Digital doctoring: how to tell the real from t5he fake. Significance, 3: 162-166.
[3] Zhu, B., M. Swanson, A. Tewfik, 2004. When seeing isn't believing [multimedia authentication Technologies. IEEE Signal Processing Magazine. Vol 21, PP: 40-49.

[4] Friedman, G.L., 1993. Trustworthy digital camera: restoring credibility to the photographic Image. IEEE Transactions on Consumer Electronics, 39: 905-910.
[5] Cox, I., M. Miller, J. Bloom, J. Fridrich, T. Kalker, 2008. Digital Watermarking and Steganography. Morgan Kaufmann. 2nd Edition.
[6] Rivest, R.L., A. Shamir, L. Adleman, 1978. A method for obtaining digital signature and public-key cryptosystems. Communications of the ACM, 21: 120-126.
[7] Farid, H., 2009. Image forgery detection. IEEE Signal Processing Magazine, 26: 16-25.
[8] Mahdian, B., S. Saic, 2010. A bibliography on blind methods for identifying image forgery.Signal Processing: Image Communication, 25: 389-399.
[9] Johnson, M.K., H. Farid, 2006. Exposing digital forgeries through chromatic aberration. In Proceedings of the 8th workshop on multimedia Security. Voloshynovskiy, S., Dittmann, J., Fridrich, J.J., Eds., pp: 48-55.
[10] Yerushalmy, I., H. Hel-Or, 2011. Digital image forgery detection based on lens and sensor Aberration. International Journal of Computer Vision, 92: 71-91.
[11] Janesick, J., 2001. Scientific Charge-Coupled Devices. Spie Press Monograph. SPIE Press.
[12] Liu, B.B., Y. Hu, H.K. Lee, 2010. Source camera identification from significant noise residual Regions in Proceedings of the International Conference on Image Processing (ICIP'10), pp: 1749-1752.
[13] Li, C.T., 2010. Source camera identification using enhanced sensor pattern noise. IEEE Transactions on Information Forensics and Security, 5: 280-287.
[14] Piva, Alessandro, 2012. An overview on image forensics. ISRN Signal Processing. Volume 2013, Article ID 496701, 22 pages.
[15] Popescu, A.C., H. Farid, 2005. Exposing digital forgeries in color filter array interpolated Images. IEEE Transactions of Signal Processing, 53: 3948-3959.
[16] Wallace, G.K., 1992. The JPEG still picture compression standard. IEEE Transactions on Consumer Electronics, 38.
[17] Fan, Z., R.L. de Queiroz, 2003. Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Transactions on Image Processing, 12: 230-235.
[18] Luo, W., J. Huang, G. Qiu, 2010. JPEG error analysis and its applications to digital image Forensics. IEEE Transactions on Information Forensics and Security, 5: 480-491.
[19] Ye, S., Q. Sun, E.C Chang, 2007. Detecting digital image forensics by measuring inconsistencies of blocking artifact. in Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '07), pp: 12-15.
[20] Lukas, J., J. Fridrich, 2003. Estimation of primary quantization matrix in double compressed JPEG images. in Proceedings of the Digital Forensics Research Conference (DFRWS '03).
[21] Ou, Z., W. Luo, J. Houng, 2008. A convolutive mixing model for shifted double JPEG compression with application to passive image authentication. in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '08), pp: 1661-1664.
[22] Fridrich, A.J., B.D. Soukal, A.J. Lukas, 2003. Detection of copy move forgery digital images. in Proceedings of the Digital Forensic Research Workshop.
[23] Mahdian, B., S. Saic, 2008. Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security, 3: 529-538.
[24] Yuan, H.D. 2011. Blind forensics of median filtering in digital images. IEEE Transactions on Information Forensics and Security, 6: 1335-11345.
[25] Sarkar, A., A. Nataraj, B.S. Manjunath, 2009. Detection of seam carving and localization of seam insertions in digital images. in Proceedings of the 11th ACM Multimedia Security Workshop (MM Sec '09), pp: 107-116.
[26] Chen, W., Y.Q. Shi, W. Su, 2007. Image splicing detection using 2-D phase congruency and statistical moments of characteristic function. in Security, Steganography and Watermarking of Multimedia Contexts IX, Proceedings of SPIE.
[27] Johnson, M.K., H. Farid, 2007. Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security, 2: 450-461.
[28] Kakar, P., N. Sudha, W. Ser, 2011. Exposing digital images forgeries by detecting discrepancies in motion blur. IEEE Transactions on Multimedia, 13: 443-452.