Anti- Forensics of Median Filtered Image using Non-Linear Optimization Techniques

Seema[1], Ms. Swati Gupta[2], Mr. Bijender Bansal[3], Dr. Deepak Goyal[4], Dr. Monika Goyal[5]

[1]M.Tech Student – Vaish College of Engineering, Department of Computer Science and Engineering, Rohtak, India

[2,3,5] Assistant Professor – Vaish College of Engineering, Department of Computer Science and Engineering, Rohtak, India

[4]Professor – Vaish College of Engineering, Department of Computer Science and Engineering, Rohtak (Haryana), India

Abstract: The growth of experienced image processing and editing software has made the manipulation of digital images easy and imperceptible to the naked eyes. This has increased the demand to assess the trustworthiness of digital images when utilized in crime investigation, as evidence in court of law and for surveillance purposes. This paper presents a comprehensive investigation of the progress and challenges within the field of digital image forensics to assist the beginners in developing the understanding, apprehending the wants and identifying the research gaps in this domain.

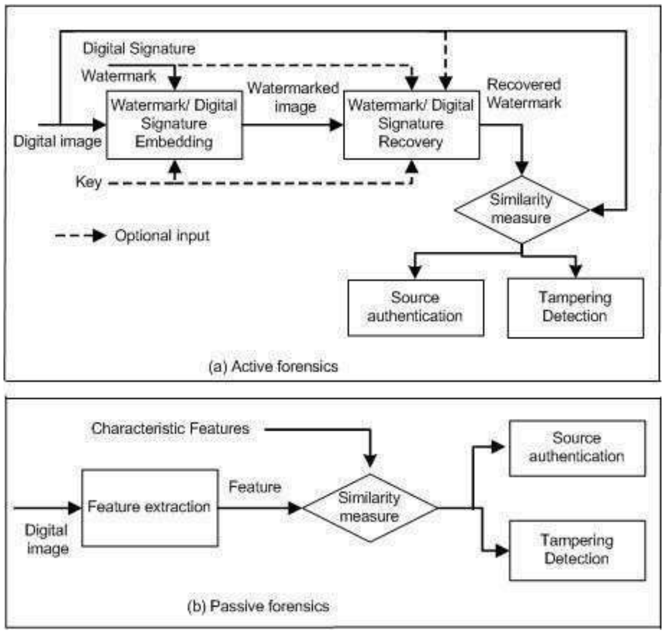
Keywords: Digital image forensics, forgery, image authentication, tampering detection, passive forensics, anti-forensics.

1. INTRODUCTION

The development and simple availability of image processing software and image capturing devices alongside the convenience of accessibility of the web has increased the ambivalence within the authenticity of the digital images [1-5]. Uses of digital images as evidence for deciding or judgments and as support for a scientific argument are examples where not only ownership of the pictures is required to be established, but it's equally important to determine their authenticity. Digital image watermarking and digital signatures are used as active approach to revive the lost trust in digital images [3]. These approaches fix some self-authenticating information within the digital media with the detached of assessing the authenticity and integrity of the digital images. Digital image watermarking belongs to the category of active approach [1-3] for image forensics because it requires the knowledge of the authentication code and therefore the method wont to embed it into the image. The hidden information is usually imperceptible and robust against most of the intended and unintended attacks like histogram equalization, compression, rotation, cropping, resampling, filtering, addition of noise etc. But, a serious disadvantage of active techniques is that they require manipulation of the first image either during capturing or during storage. Moreover, the necessity of generating the digital signature or watermark before saving the pictures involves specially equipped image capturing devices. Thus, the utilization of digital signatures and watermarking as image forensic tools isn't widely adopted [3].

Rather, passive digital image forensics [1-3] has been consider upon as the solution with the primary objective of validating the authenticity of the digital images by either detecting tampering or recovering information about their history. The passive authenticating methods are blind as these do not require the knowledge of the original image, but are based on the fact that most of the image capturing devices and image processing operations introduce distinct traces within the image generally referred to as the fingerprints [4, 5]. Passive digital image forensic methods study underlying fingerprints with respect to the two major working domains [3]. The first domain pertains to source authentication where the purpose is to identify the device used for capturing the image and reconstruct its generation process. The second realm of digital image forensicsis concerned with the detection of tampering to establish if the image has been manipulated and possibly identify the processes involved. Counterfeiting a digital image without leaving any perceptible traces is not so difficult now with the advanced and user friendly image processing and image editing software. Fig. (1) depicts the generic active and passive image forensic approach.

Fig. (1). Generic active and passive image forensic methods



This journal presents a compendious study about the progress and challenges in the area of digital image forensics and is organized as follows: Section 2 elucidates the formation of images accepting a digital camera to understand the life cycle of a digital image. Section 3 have a representation of the research aiming to identify and authenticate the device used to acquire a given digital image. Section 4 produces the major exploited prospect of research in digital image forensics domain that is, tampering detection. Section 5 sheds light on the pill for digital image forensics. Finally section 6 concludes this paper and attempts to identify major challenges in this area.

2. FORMATION OF DIGITAL IMAGES

A digital image life cycle [4, 6] can be represented in three phases: acquisition, saving and editing. During acquisition phase, the diaphragm controls the amount of light from the real scene falling onto the image sensors, the shutter speed determines the time of exposure and the lens assembly focuses the light rays to form a coherent image onto the sensors. Digital cameras [4, 7] generally use either a charge-coupled device (CCD) or a complementary metal oxide semiconductor (CMOS) as image sensor. Each sensor is made of light sensitive diodes called photosites that convert photons falling on it into electric charge proportional to the intensity of the light. Each sensor captures the data for a single picture element or pixel in the image. This will generate grayscale images because the sensors are unable to distinguish between colors. Usually, colors of an image are represented as a mixture of varying percentages of the three primary colors red, green, and blue. The color information is acquired by using a mosaic of the primary color filters known as the Color Filter Array (CFA) [7, 8]. When it is laid over image sensors, only one of the primary color that matches the characteristics of the individual filter is allowed to pass and the other two colors are blocked for an individual pixel. Thus, brightness of one color per pixel is recorded. For example, a sensor with a green filter records brightness of green light only, falling on it. The color information of the neighboring pixels is used to interpolate the other two color components that were not recorded directly. By combining these two interpolated colors with the color measured by the site directly, the full color of each pixel is calculated and the process is called interpolation or demosaicing [8]. Generally CFA uses twice as many green filters as there are red or blue filters because human eyes are more sensitive to green color. Fig. (2) shows the arrangement of color filters in a CFA, working of color filters and interpolation process to obtain raw full color image.

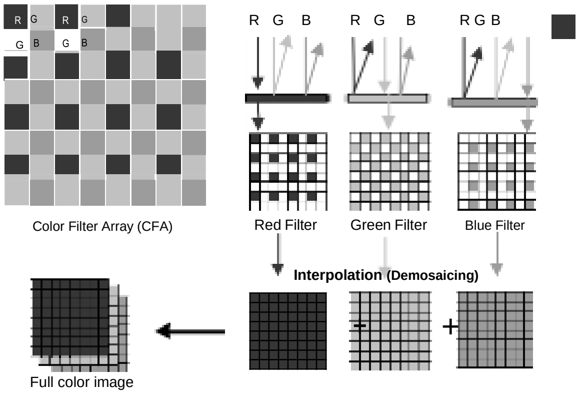


Fig. (2). Arrangement of colors in CFA, working of individual color filter and interpolation (R corresponds to Red, G corresponds to Green and B corresponds to Blue colors)

The camera thus converts light into proportional electrical charge corresponding to a color value for each pixel. But this conversion process is never perfect. For example, impurities in the silicon wafers used for making the sensors create distinctive patterns in each image which are imperceptible to the human eye. These patterns are called "photo response non-uniformity noise," which characterize the digital cameras based on the make of the sensors used. To differentiate these fingerprints from those introduced by the later stages of image life process, they are referred to as the sensor fingerprints.

The interpolated raw colored images undergo different in-camera processing operations to conceal and correct the artifacts introduced by the physical hardware depending upon the user expectations and the make or model of the camera. The general operations include linearity and dark correction, optics correction, gain non-uniformity correction, noise reduction, exposure and white balancing, color noise reduction, gamma correction and edge enhancement. The sequence of these operations may differ depending on the manufacturer. Most of these operations introduce characteristic patterns hereby referred to as operational fingerprints. This in-camera processed image with the fingerprints introduced by the sensors and the image processing operations is now ready to be saved. To reduce the amount of physical storage space required for the representation of the image, lossy compression is preferred. Many compression methods are available but Joint Photographer's Expert Group (JPEG) compression has been the choice by most of the image capturing devices. The compression method itself adds some specific fingerprints to the image hereby referred to as compression fingerprints. The compressed image is finally available for use and any further image processing operation on it is expected to alter the intrinsic fingerprints of the image and introduce new fingerprints too.

Fig. (3) summarizes the general steps during image acquisition by a digital camera with main focus on the fingerprints introduced by them.

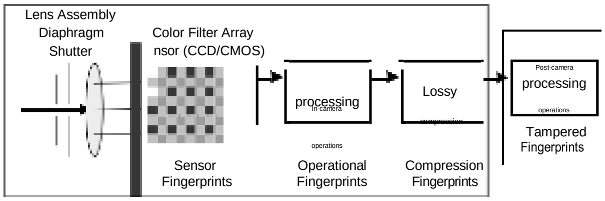


Fig. (3). General steps during image acquisition by a digital camera

3. DIGITAL IMAGE FORENSICS FOR SOURCE AUTHENTICATION OR IDENTIFICATION

Digital images can be captured by some digital cameras or scanners and can be generated on computers too. Passive image forensic techniques for source identification work on the basic assumption that the fingerprints of the imaging sensors, in-camera processing operations and compression are always present in images. Detection of camera specific fingerprints identifies the image capturing device and justify that the image is not computer rendered. The two images having the same in-camera fingerprints are judged to be taken by the same device. The absence of fingerprints in images suggests that either the image is computer generated or has been maliciously tampered thereby calling for image integrity verification. Based on the above assumptions the published works are presented in this section with respect to two issues: firstly, to distinguish between the natural and computer generated images; and secondly, to identify the image capturing device if the image is natural.

Natural or computer generated images

With the progress in computer graphics technology, sometimes, computer generated images are so realistic that they are mistakenly assumed to be natural by human perception. However, computer generated images do not fully conform to the natural image characteristics because the computer is not able to fully synthesize the complex real world phenomena.

The work presented in [9] uses linear Discrimination Analysis (LDA) and non-linear Support Vector Machine (SVM) classifiers based on first-order and higher-order wavelet statistics to distinguish between the computer generated and naturally photographed images. The image is decomposed into four-level separable quadrature mirror filters to extract the first four-order statistics of the sub-band coefficients. For every color channel of an image a 72 dimensional feature vector of coefficients and error statistics is generated. The detection accuracy of the proposed method with LDA classifier is 54.6% with low false-negative detection rate of 0.8%. The non-linear SVM classifier showed improvement in detection accuracy and was able to classify approximately 66.8% of computer generated images at the cost of increased false alarm rate of 1.2%.

A geometry-based model motivated by the physical differences in generation of the natural and computer generated image is proposed in [10] that calculate the geometric features using the method of rigid body moments, surface gradients, second fundamental form and the Beltrami flow. Other than these two image types, a third class of images used for classification in the work is the computer rendered images which are recaptured using a camera. Face authentication systems and composite image detection systems are important applications where discerning recaptured and natural image is important. Multiple feature descriptors based on local binary pattern, sensor pattern noise, difference histogram and color are extracted and compared to classify natural and recaptured images using a SVM classifier in [11] to achieve a correct detection rate as high as 97.2%.

The work proposed in [12] uses homomorphic filter to highlight image detail information. The statistical features of the contourlet sub-bands of the image are used to construct the distinguishing features for the proposed least squares SVM classifier. The proposed method is demonstrated to be accurate and robust to content preserving manipulation such as JPEG compression, noise addition, histogram equalization and filtering.

Device identification

Different imaging devices characterize different fingerprints depending on their physical hardware and in-camera processing operations and other parameters resulting in different patterns on the images captured. Fig. (4) outlines the basic process involved for imaging device identification. Assuming that the image under test has been captured by one of the candidate imaging devices, its features are extracted. These features are then compared with the characteristic fingerprints of the candidate devices and based on some similarity measure the capturing device is identified.

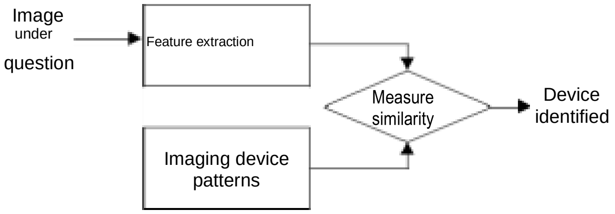


Fig. (4). Imaging device identification

4. DIGITAL IMAGE FORENSICS FORTAMPERING DETECTION

Image tampering is a deliberate attempt to add, remove or hide some important details of an image without leaving any obvious traces of the manipulation [1]. The digital images are generally tampered by region duplication, image splicing or image retouching. Region duplication is also recognized as cloning or copy-move attack, where selective regions from an image are copied, sometimes transformed, and then pasted to new locations within the image itself with the main aim of concealing some original image contents. Image splicing on the other hand uses selected regions from two or more images to be pasted together for producing a new image. Sometimes spliced images retain the majority of one image for background details. Splicing results in disturbances in the higher order image statistics. Another commonly used tampering operation is image retouching, where images with poor quality are modified for enhanced appeal.

Research is continuously going on to develop and test new tools to confirm the authenticity of digital images. Many passive blind image forensic tools have been developed to detect and locate tampering in digital images based on different principles. Fig. (5) shows the classification of passive image forensic tools [13].

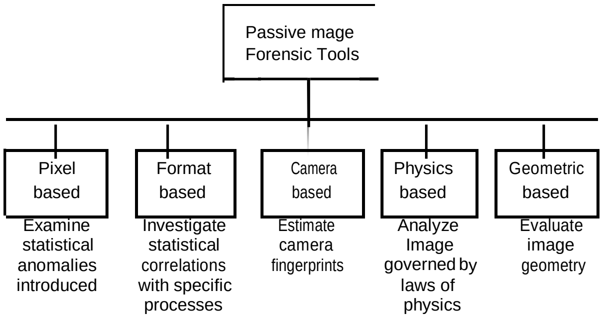


Fig. (5). Classification of passive image forensic tools

Some forensic tools rely on statistical anomalies introduced at pixel levels for detection of cloning, resampling and splicing while some other are influenced by statistical correlation introduced by specific processing like JPEG or wavelet based compression. These tools belong to the class of pixel-based and format-based tools respectively. If the image acquisition device is known, tampering can be detected using camera-based forensic techniques that detect consistency in camera specific fingerprints by modeling and estimating different camera artifacts like chromatic aberration and camera response function. It is generally difficult to exactly match the lighting direction and effects in different images even when they are captured by the same camera model. The physics-based forensic techniques estimate the properties of lighting environment, shadows and reflections of objects in the image based on relative position of the objects, texture and surface qualities. Difference in lighting across an image is used as evidence against tampering. Some forensic tools exploit the geometry of the scene and use the difference in the estimated principal points as evidence of tampering. Authentic images have their principal point near the center of the image and translation of objects in the image results in the shift of principal points.

Surveys and studies based on passive blind techniques for forgery detection [2, 5, 13-14] have focused mainly on region duplication. Cloning is difficult to be detected because the copied portion is highly correlated with the background. Manipulation of the copied region by adding Gaussian noise, scaling, rotating and using JPEG compression before pasting worsens the detection of copy-move operation further. A good cloning detection method is expected to be robust to these manipulations. General approach widely practiced by forensic experts for detecting the copy-move forgery is to divide the image into overlapping blocks and compare the features of the blocks. These techniques are called block-based techniques. Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA) etc. have been used to identify the block feature vectors in the prior works. The feature vectors are put row-wise in a matrix, which is then sorted lexicographically. It is expected that similar blocks will produce similar feature vectors which will come closer to each other as a result of sorting. An appropriate distance measure for example, Euclidean distance, with a threshold is chosen to locate the blocks which are similar. The techniques which do not divide the image into blocks but use some key points of the entire image as features are said to be key-point based techniques. These techniques use Shift Invariant Feature Transform (SIFT) and Speeded-up Robust Features (SURF) etc. to compute features from the image regions with high entropy. Thus, the block based and the key-point based techniques differ in computing the feature vectors of the image. The need to compare each possible pair of blocks makes the block-based approach costly in terms of computation time. The basic approach to copy-move forgery detection is shown in Fig. (6).

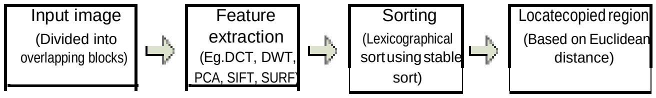

Input image
(Divided into overlapping blocks)
Feature extraction
(Eg.DCT, DWT, PCA, SIFT, SURF)
Sorting
(Lexicographical sortusing stable sort)
Locatecopied region
(Based on Euclidean distance)

Fig. (6). Basic approach to copy-move forgery detection

The two major aspects of research on the block based methods aims at reducing the time complexity and finding out the best features of the block. An attempt to save execution time of block-based approach by using a nine dimensional intensity based feature vector has been made in [15]. Each overlapping block is further divided into four non-overlapping sub-blocks as shown in Fig. (7). Top-left pixel location of each block is saved and the feature vector for each block is normalized to integers between 0 and 255 before sorting. The shift vector of the saved positions for each pair of sorted adjacent feature vectors is calculated as the difference between them. If the shift vectors are equal, it is considered as the possible presence of the duplicated region. To reduce the falsely detected similar regions, median filtering and connected component analysis is performed. The proposed features resisted Gaussian noise and JPEG compression fairly well even under rotation at specific angles. Also, use of radix sort for sorting the feature vectors instead of lexicographical sort reduced the computational time. But the work fails to detect small regions copied.

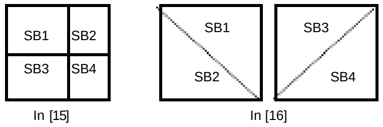


Fig. (7). Sub-blocking in [15] and [16]

The approach proposed in [15] was improved in terms of the speed and accuracy in [16] by using DWT to reduce the image resolution. This dimensionally reduced image is divided into blocks. Each block is further divided into four diagonal overlapping sub-blocks as shown in Fig. (7). Intensity based nine dimensional feature vector based on the sub-blocks is found for individual block of the image. These features are sorted lexicographically which brings the similar features next to each other. Erosion followed by dilation is performed to avoid false matching. The proposed approach was shown to be efficient in terms of processing time and gave nearly 98% correct detection of copy-move forgery in an image even under compression, Gaussian noise, scaling and rotation (up to some extent). To reduce the computational time further, multi-hop jump [17] algorithm is used to avoid unnecessary testing of the blocks obtained after using DWT to reduce the image dimensions. Fast Walsh Hadamard Transform (FWHT) is then used to extract feature of each block which are arranged as vectors before sorting lexicographically. As shown in Fig. (8) if region R is copied and pasted as R', then the block sets $\{R_m, R'_m\}$ and $\{R_n, R'_n\}$ will be at same distance. Thus testing of the second block set is unnecessary and is thus avoided.

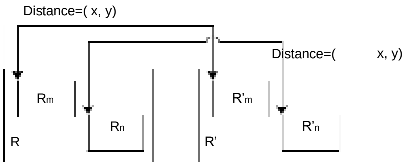


Fig. (8). Multi-hop jump algorithm [17]

The work in [18] explored the different file formats like JPEG, Bitmap (BMP) and Tagged Image File Format (TIFF) for copy-move forgery detection using a block based clustering method. The image is blurred initially to reduce the noise and image details followed by block processing. The color pattern is the feature to cluster the similar blocks on the basis of Hausdroff Distance between the colors characterizing each block of pixels. Another block based copy-move forgery detection algorithm proposed in [19] uses DWT and Principal Component Analysis- Eigenvalue Decomposition (PCA-EVD) to detect copy-move forgery in digital images. The DWT reduces the image dimension and PCA-EVD reduces the dimension of feature vector. The proposed technique detects the tampering even under JPEG compression and varying size of the copied region provided the copied region is not rotated or scaled. The feature vector of every block is found using Fourier Mellin Transform (FMT) for the work proposed in [20]. The experiments were carried out with these vectors using lexicographical sort and the notion of counting bloom filters. Instead of comparing the features directly, bloom filters compare the hashes of the features. FMT vectors proved to be resistant to scaling, translation and compression and more time efficient at the cost of some reduction in robustness. The work is shown to defeat the approach presented in [21] where specific statistical correlations introduced due to resampling are used to detect copy-move forgery for JPEG, TIFF and Graphics Interchange Format (GIF) images with minimal compression.

Some block-based methods based on ten different features and different methods of sorting are compared in [22] using a common pipeline. It is reported that lexicographic sort yields low false positive rate but exhibits severe problems when the copied region undergoes geometric transformation. FMT is found to give good overall performance if no geometric transformation is applied on the copied region and kd-tree representation [20] is used. PCA and DCT are found to give strong results even under geometric transformations when same shift vectors are used to verify matching. Another important contribution of the work is the database created and made available for researchers.

Various moments based, dimensionality reduction approach based, intensity-based, and frequency domain-based features were analyzed for block approaches against different key-point based algorithms in [23] to evaluate their performance. It is reported that SIFT and SURF methods excelled in computation time and in the conditions when the copied image undergoes several rotations and scaling operations. These methods however lack high accuracy in forgery detection when the copied image is very much self-similar. Block based methods can overcome this problem at the cost of being computationally costly. These methods perform well for Gaussian noise and JPEG compression attacks but fail to detect forgery for large rotation and scaling. The study in [23] reflected that different key-point-based methods like SIFT and SURF, and block-based methods based on DCT, PCA and DWT perform well and can be combined to get better result.

An attempt to combine block based methods with key-point based methods for copy-move forgery detection under combination of editing operations and attacks is made in [24]which is carried forward in [25] by the same authors. DCT is combined with SIFT to detect copy move forgery successfully even after post processing operations like rotation, scaling, compression and noise on the forged image in [25].

For image splicing to be done, it is often necessary to resize, rotate and/or stretch certain portions of images which requires resampling to be done. This process of resampling is always expected to introduce specific periodic correlations between pixels. This idea has been used in [26] to detect tampering. Independent Component Analysis (ICA) is explored as a tool to detect if the resultant image is a mixture of multiple images in [26] even if the image is tilted or scaled. The work requires least two versions of the image under test.

The fingerprints due to image compression are also explored by the researchers as a tool to detect tampering. The histogram of Discrete Wavelet Transform coefficients gives the fingerprints of Set Partitioning in Hierarchical Trees (SPHIT) compression, explored in [5] by looking out for any change in them for compressed and uncompressed images.

5. COUNTERMEASURES FOR DIGITAL IMAGE FORENSICS

Together with the development of forensic techniques, attempts to fool these techniques have been made by the intelligent malicious attackers. Such techniques that aim to challenge the digital forensic tools and demonstrate their limitations by removing, hiding or overwriting the characteristic fingerprints within an image are referred to as counter-forensic techniques [27]. Depending on whether a particular counter-forensic technique removes the traces detectable with a specific image forensic technique or with any unknown technique, the counter-forensic techniques are classified as targeted or universal respectively [28]. If these techniques are used in parallel with the image tampering operations, they are said to be integrated and if they are used after the manipulations it is said to be post processing. Much of the published work has focused on targeted and post processing counter-forensics with image compression as the subject [29-33].

Digital images are compressed for faster transmission and processing on the internet. Several approaches are used for the purpose and some of the popular choices include DCT and the derived tools such as JPEG, JPEG 2000, fractal image compression and wavelet transformation. These use different aspects to help image processing smoother and faster. The anti-forensic techniques surveyed in this paper aim for one of the above said methods of compression at a time. JPEG compression is found to be countered widely [30-32] based on two important artifacts introduced because of its lossy nature. First, due to quantization, DCT coefficients are closer to the multiples of the step size which is visible on the histogram of the DCT coefficients of the compressed image. This is referred to as quantization artifact. Second, blocking artifacts introduced due to pixel value discontinuities across block boundaries. Targeting to hide DCT quantization artifacts [30, 31] proposed addition of counter noise to the DCT coefficients at the cost of some distortion being introduced within the acceptable limits. The additive noise distribution is critically chosen so that the DCT coefficients are not clustered around integer multiples of the step size. The work proposed in [32] is an extension of JPEG compression anti-forensic technique presented in [30, 31] by using a bitmap image as the test image. Noise is added to the DCT coefficients based on the assumption that pixel differences within and across blocks is similar if no compression is done.

An attempt to suppress the JPEG blocking artifacts by smoothing followed by addition of low power White Gaussian noise while preserving the Laplacian distribution of the DCT coefficients has been proposed in [33]. It uses DCT coefficients histogram and blocking artifact measure to detect if an image under test has undergone JPEG compression. To fool the forensic examination, it was proposed to add anti-forensic dither to the DCT coefficients after initial JPEG compression but before the second pass of JPEG compression. This will reflect as if the image has been obtained directly from a digital camera and has undergone JPEG compression within the camera just once.

JPEG compression has been in the market since a while and has been explored by forensic and anti-forensic researchers considerably. To avoid the easy detection of compression fingerprints new compression methods are being evolved and expected to be used by the camera manufacturer’s as an alternate to JPEG compression. Wavelet-based compression technique is getting popular now days because better compression is achieved without loss of much detail. Additionally, since wavelet-based compression techniques do not divide the image into blocks but analyze the entire image, no blocking artifacts are produced. But the characteristic fingerprints of the technique are present which can be removed by adding anti-forensic dither to the wavelet coefficients of the compressed image as presented in [34]. The dither is added to highly textured blocks of the compressed image so as to match the coefficient distribution of the uncompressed image.

Not only compression has been studied for anti-forensics but median filtering is studied too. Median filtering is characterized by the basic idea that probability of adjacent pixels being similar is high. In other words, the difference between the adjacent pixels after median filtering is more likely to be zero. The median filter is a typical pre-processing step to improve the results by removing noise while preserving edges. The characteristics of median filtering are measured using five different features [35]: distribution of block median; occurrence of block center gray level; quantity of gray levels in a block; distribution of block center gray level in sorted gray levels and first occurrence of block center gray level in sorted gray levels. The work presented in [35] hides the characteristic traces of median filtering in uncompressed images by modifying suitable random pixels based on the occurrence of block center gray-level and distribution of block median. Smooth blocks are expected to have block center value occurring more frequently and high probability of having more than single median value within a block. So the blocks with high values for distribution of block median and occurrence of block center gray level are discarded and a random small perturbation is added to those blocks amongst the rest which have standard deviation higher that an empirical threshold. Another approach to conceal traces of median filtering has been presented in [36] which use linear convolution filters of size 3×3 to produce another image from the median filtered image such that the fidelity between the median filtered image and that obtained after convolution filtering is maximized.

A survey on anti-forensics operation has been presented in [37, 38].

Countering Anti-Forensics

The use of anti-forensics by the forgers to hide the tampering has resulted in the study of fingerprints that might be introduced due to their use. Many counter-forensic techniques have been developed to hide JPEG compression artifacts [30-32]. The fingerprints left by these techniques themselves have been explored and the work presented in [39] hided them based on the inter- and intra-block correlation. Not only counter JPEG compression but anti-forensic techniques for wavelet-based compression have been studied for their characteristics. Counter anti-forensics for wavelet based compression techniques is presented in [40]. The fingerprints of counter-wavelet-based compression are suppressed by analyzing relations between DWT coefficients across different levels. Hough transform is applied to the joint DWT histogram to derive the feature vector using a Support Vector Machine (SVM). A short review of anti-forensics for median filtering is presented in the last section of the paper which is countered by the work presented in [41]. To detect the fingerprints of anti-forensics for median filtering, the difference between adjacent pixels in horizontal direction is determined using which ratio of zero for each row is found. If discrete Fourier transform of these ratio of zero for each row exhibits periodicity, it is expected to confirm that the image has been modified by an anti-forensic method.

An attempt to detect anti-forensic operation performed on spliced JPEG image has been made in [42]. The decision to confirm tampering is based on the forensic and counter-anti-forensic analysis of the image. The forger is assumed to hide the traces of splicing using two anti-forensic tools for the work and the image is classified as tampered if either of the tools identifies the fingerprints of tampering or anti-forensic operation. JPEG compression is mostly studied to identify the traces of compression.

6. CONCLUSION

With the outgrowth of the imaging and communication technology, the exchange of digital images has become easy and extensive. But at the same time, the instances of manipulations in the digital images have also increased thereby resulting in greater need for establishing ownership and authentication of the media. Digital image forensic researcher community is continuously attempting to develop techniques for detection of the imaging device used for image acquisition, tracing the processing history of the digital image and locating the region of tampering in the digital images. The sensor, operational and compression fingerprints have been studied with various image features to achieve the purposes. An attempt to recover the tampered region details is expected to be an appealing investigation domain for many researchers. Due to format incompatibility and use of encryption many organizations find their data to fail to qualify for analysis using many of the existing techniques. So, the need is to develop not only robust forensic techniques but these should be format independent and take encryption into consideration too.

The war between the forensic researchers and malicious attackers is never ending and the result is an almost equal growth and development of anti-forensics techniques aiming to reveal and exploit the weakness of forensic technology. So, anti-forensics techniques are required to be studied and explored to understand which forensic techniques can be deceived. Also researchers need to study if these techniques themselves leave behind some fingerprints which can be used to detect the use of anti-forensic operations. This will reduce the probability of falsely classifying the anti-forensic processed images as the true images and thereby increasing the reliability of the existing and new forensic techniques. Anti-forensics can also be looked upon as a tool to protect reverse engineering. Most of the work done in image forensics has focused on detecting the fingerprints of a specific kind of tampering operation. But, practically a manipulated image is often the result of multiple such tampering operations applied together. Thus, the need is to develop a technique or framework capable of detecting multiple attacks and tampering.

REFERENCES

[1] Cheddad A. Doctored Image Detection: A Brief Introductionto Digital Image Forensics. Inspire magazine, July 2012.

[2] Qazi T, Hayat K, Khan SU, Madani SA, Khan IA, Kołodziej J, Li H, Lin WYKC, Xu CZ. Survey on Blind Image Forgery Detection. IET Image Processing 2013; 7(7), 1–11.

[3] Guojuan Z and Dianji L. An Overview of Digital Watermarking in Image Forensics. In: Proc. of 4th IEEE International Joint Conference on Computational Sciences and Optimization, 2011, pp. 332-335.

[4] Swaminathan A, Wu M and Liu KJR. Digital Image Forensics via Intrinsic Fingerprints. IEEE Trans on Information Forensics and Security 2008; 3(1), 101-117.

[5] Weiqi L, Zhenhua Q, Feng P and Jiwu H. A Survey of Passive Technology for Digital Image Forensics. Review article, Front. Comput. China 2007.

[6] Abhitha E, Karthick VJA. Forensic Technique for Detecting Tamper in Digital Image Compression. International Journal of Advanced Research in Computer and Communication Engineering 2013; 2(3), 1325-1330.

[7] www.cambridgeincolour.com/learn-photography-concepts.htm

[8] Kirchner M. Efficient Estimation of CFA Pattern Configuration in Digital Camera Images. SPIE 2010; 7541.

[9] Lyu S, Farid H. How realistic is photorealistic?. IEEE Transon Signal Processing 2005; 53(2), 845-850.

[10] Ng TT, Chang SF, Hsu J, et.al. Physics Motivated Features for Distinguishing Photographic Images and Computer Generated Graphics. In: Proc. of ACM Multimedia November 2005; 5, 239-248.

[11] Ke Y, Shan Q, Qin F, Min W. Image Recapture Detection using Multiple Features. International Journal of Multimedia and Ubiquitous Computing 2013; 8(5), 71-82.

[12] Wang X, Liu Y, Xu B, Li L, Xue J. A Statistical Feature Based Approach to Distinguish PRCG from Photographs. Computer Vision and Image Understanding 2014; 128, 84-93.

[13] Farid H. Image Forgery detection- A Survey. IEEE Signal Processing Magazine 2009; 16-25.

[14] Bayram S, Sencar HT, Memon N. A Survey of Copy-move Forgery Detection Techniques. Unknown 2008.

[15] Lin HJ, Wang CW, Kao YT. Fast Copy-Move Forgery Detection. WSEAS Trans on Signal Processing May 2009; 5(5),188-197.

[16] Singh VK, Tripathi RC. Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method. International Journal of Advanced Science and Technology 2011.

[17] Yang B, Sun X, Chen X, Zhang J, Li X. An Efficient Forensic Method for Copy–move Forgery Detection Based on DWT-FWHT. Radioengineering December 2013; 22(4), 1098-1105.

[18] Chaitawittanun N. Detection of Copy-Move Forgery by Clustering Technique. In: Proc. of International Conference on Image, Vision and Computing 2012; 50.

[19] Zimba M, Xingming S. DWT-PCA (EVD) Based Copy-move Image Forgery Detection. International Journal of Digital Content Technology and its Applications 2011; 5(1).

[20] Bayram S, Sencar HT, Memon N. An Efficient and Robust Method for Detecting Copy-move Forgery. In: Proc of ICASSP2009.

[21] Popescu AC, Farid H. Exposing Digital Forgeries by Detecting Traces of Resampling. IEEE Transactions on Signal Processing 2005; 53, 758–767.

[22] Vincent C, Christian R, Elli A. A Study on Features for the Detection of Copy-Move Forgeries. In: Proc. GI SICHERHEIT 2010; 105 -116.

[23] Vincent C, Christian R, Johannes J, Corinna R, Elli A. An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Trans on Information Forensics and Security 2012; 7(6).

[24] Kaur A, Sharma R. Optimization of Copy-Move Forgery Detection Technique. International Journal of Advanced Research in Computer Science and Software Engineering 2013; 3(4),576-578.

[25] Kaur A, Sharma R. Copy-Move Forgery Detection using DCT and SIFT. International Journal of Computer Applications May 2013; 70(7).

[26] Kumar S, Desai JV, Mukherjee S, Das PK. Suitability of Independent Component Analysis in Digital Image Forgery Detection. International Journal of Engineering and Technology Feb-Mar 2013; 5(1), 226-231.

[27] Rainer B, Matthias K. Counter-forensics: Attacking Image Forensics. Digital image forensics-Springer 2012.

[28] Matthias K, Rainer B. Tamper hiding: Defeating image forensics. Information Hiding, ser. Lect. Notes Comput. Sci. 4567, T. Furon, F. Cayre, G. Doërr, and P. Bas, Eds. Berlin, Germany: Springer-Verlag, 2007; 326–341.

[29] Stamm MC, Liu, Ray KJ. Anti-Forensics of Digital Image Compression. IEEE Trans on Information Forensics and Security September 2011; 6(3), 1050-1065.

[30] Matthew CS, Steven KTW, Sabrina L, Ray KJL. Anti-forensics of JPEG Compression. In: Proc. of IEEE Conference on acoustic, speech and signal processing March 2010.

[31] Sreelakshmi MS, Venkataraman D. Image Compression Using Anti-forensics Method. International Journal of Computer Science, Engineering and Applications 2013; 3(1),81-89.

[32] Manimurugan S, Athira BK. A Tailored Anti-forensic Technique for Digital Image Applications. International Journal of Computer Applications 2012; 53(9).

[33] Matthew, CS, Steven KT, Sabrina L, Ray KJL. Undetectable Image Tampering Through JPEG Compression Anti-forensics. In: Proc. of 2010 IEEE 17th International Conference on Image Processing, Hong Kong, 2010.

[34] Matthew CS, Ray KJL. Wavelet-based Image Compression Anti-forensics. In: Proc. of IEEE 17th International Conference on Image Processing, Hong Kong, 2010.

[35] Dang-Nguyen DT, Gebru ID, Conotter V, Boato G, De Natale, FGB. Counter-forensics of Median Filtering. In: IEEE 15th International Workshop on Multimedia Signal Processing, Italy, 2013.

[36] Fontani M, Barni M. Hiding Traces of Median Filtering in Digital Images. In: European Signal Processing Conference, Romania, 2012.

[37] Pranita DP, Monika R. Survey on Anti-Forensics Operations in Image Forensics. International Journal of Computer Science and Information Technologies 2014; 5(2), 1570-1573.

[38] Singh N, Joshi S. Digital Image Forensics and Counter Anti-Forensic. In: Proc. of International Conference on Recent Cognizance in Wireless Communication and Image Processing, January, 2015.

[39] Li H, Luo W, Huang J. Countering Anti-JPEG Compression Forensics. In: Proc. of 19th IEEE International Conference on Image Processing 2012.

[40] Wang M, Chen Z, Fan W. Xiong Z. Countering Anti-Forensics to Wavelet-Based Compression. In: Proc. of the IEEE International Conference on Image Processing (ICIP), Paris, France, October2014.

[41] Zeng H, Qin T, Kang X, Liu L. Countering Anti-Forensics of Median Filtering. In: IEEE International Conference on acoustic, speech and signal processing, 2014.

[42] Fontani M, Bonchi A, Piva A, Barni M. Countering Anti-Forensics by Means of Data Fusion. In: Proc. of SPIE Electronic Imaging conference, 2014