Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY OF COPY-MOVE FORGERY DETECTION TECHNIQUES

[1,2] SALAM A.THAJEEL, [1]GHAZALI SULONG
[1] UTM-IRDA Digital Media Centre (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia (UTM), 81310 UTM Skudai, Johor, Malaysia
[2] Computer Science Department , Collage of Education , University of Al-Mustansiriyah, Baghdad, Iraq
E-mail: [1] sath72@gmail.com, [2] ghazali@utmspace.edu.my

ABSTRACT

Copy-Move forgery is one of the significant image manipulations, where some image parts are copied and pasted in original image. In this survey, we firstly review about digital image forensics and its types. The brief discussion about current research presented here with an analysis of the existing approaches for detect image tampering, which are classified into block-based method and key point-based method. Then we demonstrate the popular techniques of two methods and analysis of several techniques. Finally, the all techniques advantages and disadvantages summarized and some future research directions were pointed out.

Keywords: *Block Matching, Digital Image, Forgery Detection, Copy-Move Forgery,*

1. INTRODUCTION

Digital image play a significant role in different technologies and fields. The use of digital cameras, personal computers, and sophisticated image processing software available for modification and for manipulation of image. These tools are scalable and provides user interface features. An image can be manipulated easily through image-processing tools and use for hiding some meaningful or useful information to make forged images [1]. The basic aim of image forensics to address image integrity and authenticity. Image slicing, cloning, tempering has been done to make forged images and integrity of image is lost. These digital forged images are not recognizable and so real and authenticity is lost. Therefore, integrity and authenticity verification of digital image has been gain researcher attention in image processing field. The various types of tools widely used for tamper and maliciously manipulate digital images such as Freehand and Photoshop etc. Therefore, developing techniques to verify these digital images became very important especially when images are used for any law proceedings in court, for medical purposes and financial document, transportation sector etc[2-4]. The digital forgery detection techniques have been proposed to deal with different types of tampering images and determine the image authenticity and trustworthiness [5]. In recent times, several authors worked and analyzed the issues of detecting image forgeries; and presumption the tempered images and cannot expose anomalies and any visual, the essential information of tempering images compare with original images [6, 7].

This survey deals with digital image forensics and their types and main focus on copy move forgery (image manipulations). The survey prearranged as follows: section 2 defines the digital image forensics and their types; in section 3 explanations about copy-move forgery detection and their techniques: section 4 discusses the challenges and issues in copy-move forgery and its types.

2. DIGITAL IMAGE FORENSICS

The three major determinations of Digital Image Forensics are; Detection, source identification of digital Image, and Image Forgery Detection. The Detection of Computer Generated Image is very hard and difficult because of its high quality and high realism realistic make confusion for viewers to judge reality [8]. In image source, identification the digital device determines like cameras, and scanners. Every device have distinctive footprint of image. In this type of forensics two approaches use in first method the image source identification attempt to resolve the source image class properties [9, 10], and second method identify the image potential source device through novel hardware characteristics [11, 12]. In

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

last, the Forgery Detection is an intrusting method for digital image forgery. The forgery detection has algorithms and techniques for detection and traces image tampering. The traces are used for proof of tampering.

The various types of algorithms and approaches have been proposed for tempering image detection and categorized into two types: active and passive. In active group the inside image and modification information are used, which are dispersed before such as watermarking and digital signature. The watermarking is inserting in the image at the time of capture, and then verifying the integrity of the mark at the recipient. The digital signatures consist of take out exclusive characteristics of image from camera, and encoding them into a signature it depends on application [13, 14]. The hidden data in watermarking may be robust, fragile or semi-fragile [15-17]. In robust watermarking, watermark stands with the image even after processing like translation, scaling, rotation, and compression and protect the copy right of digital media. In fragile watermarking, the slight change or modification on the image may lead to invalid image and authenticity of image can be verified. Whereas semi fragile watermarking is used to distinguish between malicious (modification, cropping etc.) and non-malicious attacks (compression, smoothening etc). One of the major limitation in active approach is watermark or signature inserted when capturing image or by an authorized system. This requirement of specialized hardware narrows the fields where these approaches are applicable. Additionally, the presence of hidden data may degrade image quality in some cases. The second type is passive method used for detect the forgery image traces but without guarantee that image pass the test or not. This type does not require any sort of prior information and work purely on binary data. The detectable traces are authentic and has not been modified in image [18].

2.1 Types of Digital Image Forgery

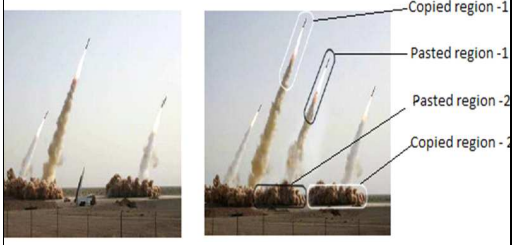
Fake images have become widespread in society today. Therefore, the tampering images are common in scandal, controversies. One can find forged images used to sensationalize news, spread political propaganda and rumors, introduce psychological. As the credibility of images suffers, it is necessary to devise techniques in order to verify their genuineness and trustworthiness of images [5].

The forgeries are classified into five major categories: image retouching, Image Splicing, Copy-Move (cloning), Morphing, Enhanced. The first type is image retouching, where the method is used for enhances an image or reduces certain feature of an image and enhances the image quality for capturing the reader's attention. In this method, the professional image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing. The second type is image splicing where the different elements from multiple images are juxtapose in a single image to convey an idea. The idea is not reflect reality. Such splicing can usually be detected by searching the splicing boundary (or the effect of the splicing on image statistics), or by considering the directions of the light incident on surfaces in the image. Other abnormalities such as inconsistent demo saicking or chromatic aberration may also be used to determine the authenticity of such images. Inconsistencies in lighting or blurred splicing boundaries can be used to expose the above images as fake, if the light direction can be correctly estimated or if the splicing boundary can be correctly detected respectively [18]. The third type is copy-move attack and same like image splicing because in both techniques modify the image area to use other images. The some portion of base image uses in copy-move attack instead of external image as a source. The parts of base image copy and move to modified image and pastes. This method usually for hide definite particulars or to matching convinced features of an image. The blur tool is use for retouching borders and decrease the effect between original and pasted area [19]. Copy-move forgeries are usually detected by searching for matching regions in the image, although recent research has taken a more feature-based approach, concentrating on matching features (as in object detection) rather than blocks, in order to allow for various image transformations that can be used to create more convincing forgeries. The forth type is Morphing and in this type the image and video can be exposed into unique influence ,were the one object on image is turned into to another object in the other image. The morphing is used to transfer the one-person image from another person image by using seamless transition between two images.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1.1: Types of Digital Image Forgery

Types	Detail	Appearance
Image retouching,	An example of forgery where the original image and a forged image shows the difference [19].	
Image Splicing,	In these images some parts of image copy from base image like shark. The base image (helicopter rescue) first turns over horizontally and the shark image is pasted to make new forged image. The forged image is not splicing with the original helicopter rescue image [20].	
Copy-Move (cloning),	The images shows the copy-move attack and in left side image three rockets and in The forged image contains four rockets [21].	
Morphing,	The left and right images are original the middle image is -morphing image [19].	
Enhanced	The original image is upper right side and after that enhanced image with color change, after perform blur on background, finally original image (lower right)Current .	

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The digital image can easily save into various types like, SWF, GIF, JPEG, and other popular formats, and can be use any software to see the result whenever required. In past the image morphing was difficult but now many software help the user to perform the job simply such as, Sqirlz Morph, FotoMorphFreeMorphing etc. The last type is based on enhancement in an image with the help of Photoshop such as situration, blur and tone etc, these enhancment cannot effect on image meaning [20]. The Table 1.1 shows all types of images with detail.

3. COPY/MOVE FORGERY DETECTION

The techniques for digital forgery detection have been proposed to solve the issues related with forgery in image processing [23]. Many studies were conducted to improve the techniques for copy-moving forgery [24], like adding or hiding a region and show incorrect information [25].

3.1 Current Challenges and limitation

The main challenges are categorized into five types: natural, forgery detection, flow mapping, and source identification. The first category natural deal with signature, author description, tags etc, and uses these information for authenticity and originality of image. However these information lead to forgery and become an issue in several cases [26-27]. The second main category of current challenges is forgery detection. Now days the many digital software tools are available for editing or alteration and easy to handle and use. This is one of the reason to detect forgery is very complex and threatening problem [28]. The third type flow mapping delivers some extra information about forgery source, where copied areas marked and used for recognizing the pasted area in the same image. The availability of software tools and some complications to recognize the area of source image and fast internet accessibility enhances the challenges of validity of digital possessions [29]. The flow mapping category deals with these forgers and rely on in copying and pasting areas [30]. Then some features are found because of new types of image achievement devices for example scanner, digital camera and cell phones, etc. To address these challenges various techniques have been proposed to handle forgery images.

The different types of techniques proposed to handle copy move Forgery but still have many limitations on detection performance, in detect rotated duplications etc.

In order to evaluate and compare the existing techniques in copy move Forgery, we picked the two groups: block based and key-point based methods briefly discuss in below section.

3.2 Existing Techniques

The copy move forgery detection (CMFD) practically divided into two main groups block based methods and Key-point-based method as shown in Figure 1.2.

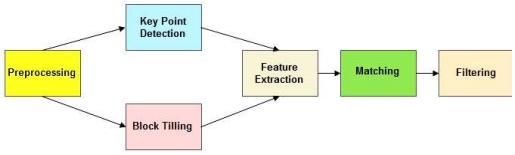


Figure 1.2: CMFD classifications

3.2.1 Block-based methods

Many techniques are based on block-based scheme where image separated into small overlapping or non- overlapping blocks. Then the separated blocks compare with each other for analyzing the matching areas and these areas cover through matching blocks.

a) Moment-based Techniques

In Blur Movement, technique the author [31] used blur property for invariants of image areas due to non-effected by means of blur additive noise and degradation. In this method the process started from tilting of image blocks of a specific size and blur invariants with every block. The every each size is 72 in length in feature vector. These are stabilized for more enhancements of the repetition recognition capabilities. The chief component transformation (PCT) is applied to decrease the feature vector dimension. In blocks for similarity analysis k-d is used as a tree representation. The used of certain threshold value for identifying same blocks and verified. The verification process possible via through finding similar blocks identical neighborhood. If there are two similar non-identical neighborhoods measured as an incorrect positive. The proposed method detected blurred duplicated region for images and detect duplicated regions which are changed contrast values. The one of the main issue in this method is computation time is comparatively high.

In Hu movement based technique the author [32], used Hu moments and deal robust to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

several post-processing methods like lossy JPEG compression and blurring. The technique decrease the dimensions through Gaussian pyramid of the image. The image separated into many fixed sized blocks that and further coinciding and calculate the reign values through Hu moments. Further arranged these vectors lexicographically and decrease false detections. The mathematical morphological techniques performed for finding matching blocks. This approach is efficient for perceiving copy-move forgery. The SIFT movement technique author [33] proposed for perceiving image copy-move forgeries through SIFT and Zernike moments. The purpose of SIFT algorithm is perform normal detections. However, the algorithm not detects flat copied regions. The procedure starts from SIFT features points extraction and used these feature for conceivable matches. To deal with false alarms of forgery, the hierarchical clustering is used and via clustering feature points converts into a tree structure and based on definite threshold value. The proposed technique decreases false alarms because the image is forged only when three similar feature points matched. Though, the method decreases the option of detecting flat forgeries.

b) Dimensionality reduction-based Methods

In PCA dimensionality reduction based technique author proposed [34], a technique and used PCA (Principal Component Analysis) for forgery image. This approach is same like DCT method and improved in capturing discriminating features. In this method the image transformed into grayscale and separated into many parts, which are represented into vectors. These parts or blocks are organized it lexicographically earlier matching and used PCA to represent the dissimilar blocks in an substitute mode. It is proficient for detection even minor variations because of noise or lossy compression. However the proposed technique is for grey scale images and also processes every color channel in color images and PCA is for detection the counterfeits. The proposed method is better for detecting copy-move forgeries and gives less number of false positives.

Another proposed method is Singular Value Decomposition (SVD) [35], and robust to post-processing techniques and computationally is less complex. In this method the correlation is used for copied and pasted areas and for searching equal regions. In this proposed method the image is separated into many small overlapping blocks and then SVD is applied for extracted exclusive single significance feature vector. The vectors initiate the similar blocks through altering every block into k-d tree. Further the method used the threshold value to rise to eliminate pseudo-matching and robustness. The natural image is without duplicate area with comprehensible alignment. The achieve match blocks indicate to copy-move forgery. The proposed method failed to detect copied and pasted block out of two matched blocks and not vigorous in contradiction of JPEG compression.

In another technique [36] the two methods used: DWT (Discrete Wavelet Transform) and KPCA (Kernel Principal Component Analysis) for copy-move forgery detection. The image is separated into many parts and for every block calculated DWT vectors and KPCA-based vectors. After this calculation these vectors sorted its lexicographically and search the related points and again intended their offset frequencies. To deal and evade with false findings a threshold located the worth for offset-frequency. Then a new algorithm developed for detection rotation type and flip of forgeries and for geometric transformation using labeling technique. The proposed approach showed betterment, if compare with conventional PCA-approach. Further it is detect forgeries, with lossy JPEG conversation and an additive noise.

In this technique author [37] proposed approach used DWT. The process initiates from color image conversion into grayscale and applied DWT to whole image. Through this the sub-bands achieve detection method. The image is divided into many coinciding blocks and achieved Principal Component Analysis – Eigen Value Decomposition (PCA-EVD). Then placed these feature into sorted the entries lexicographically and matrix. The matching is less complex in this method. The shift vector and normalized shift vector are calculated and then offset frequency and imperiled to morphological processing for final results. The proposed approach is most effective compare to conventional PCA. Because the method decreasing the size of image in start of the process. Further the method detects duplications and rotation comprised morphological operations to circumvent false detections. In this method one drawback is repetitive are as are superior compare to block size. Further the method failsin detection forgeries like rotation,heavy compression and scaling.

c) Intensity-based Methods

In this type of methods one proposed method [22]based on intensities and separated into

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

many coinciding blocks. After division the blocks split into four directions and two equal parts. The divided each block features of vector and computed the blocks which are using Additive White Gaussian Noise (AWGN) operation and lexicographically sorted. The group of same blocks feature vectors not characterize as a repeated area of image. Consequently, the approach has to be established to regulate pairs, and shows the duplicate are as to use shift vector technique. The proposed method is lower computational and compound and vigorous to post-processing operations. Whenever the forged areas are superior with block size the method is well and fail when the images are large smooth regions and highly distorted.

In another method [23] the Guassian pyramid are used for image dimensions for circle block and analyzed four features. These features are lexicographically sorted by using a convinced threshold value and search matching feature vectors. From this method the detection is effectively work by regulating threshold value, and matching feature vectors controls. This method applied on tampered images with post-processing like blurring, rotation and lossy JPEG compression. The process is better in improved the efficiency and in fine down the number of block-matching search space.

Another study proposed by [21]used to complete copy-move forgery detection in real-time. Other approaches have high computation time and not suitable for real time applications such as PCA, DWT, or SVD. The proposed approach started from separated the grayscale image into many overlapping blocks of a definite size and intensity features for every block are extracted. The two locations of the feature vectors store the block position. In this method the performance is better compare to other conventional techniques. This performance possible through reduce the processing time. The approach is also control the false detection rate through adjusting the block size. Though, the method is not for color images.

d) Frequency-based Methods

In this frequency based method author [24] proposed a DCT-based approach for multiple copy-move forgery such as noise contamination Gaussian blurring and rotation up to angle 5 degree. In this method, the authors suggested convert the RGB image to YUV and separated divided the Red, Blue and Green channels, and Y-component into fixed sized blocks. The DCT coefficients are calculated over every block in order to extract features and arranged into matrix. The matrix is lexicographically sorted, and then the matching is functional.

Another study [25] conducted used Fourier-Mellin Transform (FMT) because of its blurring, robust to lossy JPEG compression, scaling, noise and translation effects. The image is divided into many tiny sized blocks and premeditated the Fourier transform of every block. Through this transform is translation invariant and then re-sampled, quantized and projected to get feature vectors. These vectors are finished rotation invariant to small rotation angles and matched to find same feature vectors through counting bloom filters and Lexicographic sorting. Even a natural image can have numerous same blocks. The approach could detect forgeries, which are involved in blocks and rotations up to 10 degrees and a scaling of 10% and robust to JPEG compression as well.

In another technique for copy move forgery proposed by [26]to detection using Multi resolution Local Binary Patterns (MLBP). The images (RGB) are converted to gray scale and used standard color space transformation and then the input image separated into overlapping blocks. The results showed that this filtering has effective enhancements on detection presentation. Afterward MLBP is functional to each block to extract the features. In [27]proposed method works on chrominance channels rather than RGB channels so first convert RGB image to YCbCr. Undecimated wavelet transform (UWT) is used to crumble an image into dissimilar frequency bands, and a new multi-scale Weber pattern (WP) is applied on the lowest frequency sub band. The WP histogram is fed into a provision vector machine (SVM) classifier to determine the forgery. The projected method does not calculate similarity between the objects in the image, nor does it estimate the weak sensor noise pattern.

3.2.2 Key point-based Methods

In this method the author [28], proposed a method and take some advantages from correlation among the pasted region and original image area. The method also presented SIFT (Scale Invariant Feature Transform) algorithm for detailed detection and robust in contradiction of post processing. The method calculated SIFT key points and matched with another to find forgeries. If the result is in the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

shape of identical SIFT points and further image declared as copy-move forgeries. The matching procedure was done for every key point by classifying its nearest neighbor. The threshold value is ratio of closest neighbors. To enhance the strength of the method some difficulties faced during implemented in high scale images. To solve this problem used BBF (Best-Bin-First) search method resulting from k-d algorithm, for matching. The technique classifies the greatest related vectors with maximum prospect and minimum calculation. Then take one tempered image and repeated the detection for dissimilar threshold values and initiate that the accuracy of detection is reliant on on it. An optimum threshold value has to be select to test the sturdiness by effectively perceiving forgeries in a tampered image with post-processing. The proposed technique is effective in using SIFT algorithm to detect the copy-move forgery and robust for post-processing. However, the technique has problem when the SNR value is low and tampered region is small.

The author [29], proposed a method and used Speeded up Robust Features (SURF) algorithm. In this method Hessian matrix is used for the key point detection and description and for assigning the orientation. The projected dominant orientation and defined the orientation of the interest point descriptor. The Haar wavelets are invariant to the illumination bias. Then the SURF descriptors used for matching. The threshold is used to enhance the robustness and evade false detections. Then the author tested this method on different images and results shows the successful results.

4. OTHERS METHODS

The copy-move masking is first approach proposed by [30] through re-touching. The [31] algorithm proposed for detection and based on a nearest neighbor search and filtering operation, also it detect traces of tools image such as Adobe Photoshop Poisson cloning and healing brush. The proposed algorithm is use image as a graph and separated into intensity segments and appropriately weighting.

Another MPEG-7 image signature tool adopted by [32] for detect copy-move forgeries. In this signature tool the MPEG-7 standard, proposed for fast and robust image and video retrieval. The algorithm was difficult but can reduce FPR values because of stringent multi-hypothesis matching. Though, the author did not showed robustness in results. Another new approach[33]based on copied paste regions idea with same noise pattern. The proposed solution depends on image segmentation and noise estimation for each segment. Therefore, the first steps is using multi-scale segmentation algorithm in order to input image segmentation. The method algorithm works with multiple scales of image in parallel, without iteration, to detain mutually coarse and fine level details. This segmentation algorithm works concurrently crossways the graph scales, with an inter-scale restriction to make sure communication and steadiness between the segmentations at each scale. After this use statistical properties in order to estimate image noise. And finally analyze noise pattern of each segment. The image is tampered if the noise patterns of at least two segments are similar.

5. OPEN RESEARCH ISSUES

The copy-move forgery detection is one of the main problems in digital image forensics. Further there are two open research issue identified during this study robustness against geometric transforms including rotation, scaling and time complexity especially in image quality. Hence there is a need for efficient technique to handle these issues.

Below table 1.2 shows the all techniques which are discussed in this survey with their methodology and advantages and disadvantages.

6. CONCLUSION

The copy-move forgery detection is one of the main problems in digital image forensics. Several methods and approaches have been proposed to deal with these problems. There are two major challenges: robustness against geometric transforms including rotation, scaling and time complexity especially in image quality. We discussed the digital image forensics and its types, challenges and research problems and detail analysis of the existing approaches for detect image tampering. We also discussed block-based method and key point-based method and popular techniques of two methods. Moreover, most of the methods may not address the problems. Therefore, there is a need to develop techniques that is efficient to deal with these challenges. Therefore, how to merge these two techniques is future research direction.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1.2: Copy/move forgery Techniques with advantages and disadvantages

	Author/Year	Methodology	Advantage	Disadvantage
1	Mahdian,2007, [34]	BLUR	Duplicated regions detect with changed contrast values and blurred regions can also be detected.	High computation time of the algorithm.
2	Wang,2009, [35]	HU	Robust and efficient method, detects post-processing effects like noise addition, blurring, lossy compression etc.	Many False positives
3	Mohamadian,2013 [36]	ZERNIKE	Flat regions of forgeries are detected.	Calculating Zernike moment coefficients is complex
4	Popescu,2004, [37]	PCA	Efficient method, low false positives.	Low efficiency for low quality of image, low SNR and small blocks.
5	Ting, 2009, [38]	SVD	Can detect duplication even post-processing is done, robust and computationally less complex.	Cannot detect copy paste regions
6	Bashar, 2010, [39]	KPCA	Can detect additive noise and lossy JPEG conversation.	Average precision is less than wavelet based methods 'precision.
7	Luo,2006, [22]	LUO	Low computational complexity and robust to post-processing operations.	Cannot work on highly distorted images and images with large smooth regions.
8	Wang, 2009, [23]	CIRCLE	Working for post-processing like blurring, rotating, noise adding etc.	Scaling and geometric transformations cannot be detected.
9	Sridevi, 2012, [40]	PCMIFD	Extracting features and sorting are done in different algorithms in parallel, less computational time, good for real-time applications.	Not applicable to color images.
10	Fridrich, 2003, [41]	DCT	False matches are reduced by considering matching of mutual pairs as well.	Can give false positive when the image has large identical textures.
11	Bayram, 2009, [25]	FMT	Efficient and robust to blurring, noise, scaling, lossy JPEG compression and translational effects.	Cannot detect forgeries, which have rotation of above 10 degrees and scaling of 10%.
12	Qiao, 2011, [42]	CURVELET	Multi-dimensional and multi-directional gives precise results.	Cannot be applied on compressed images.

ACKNOWLEDGMENTS

The authors are thankful to the Ministry of Higher Education (MOHE) in Iraq for providing a research grant and also to Universiti Teknologi Malaysia (UTM) for providing the necessary facilities for the preparation of the paper. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, to improve the presentation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] Q.-C. Yang And C.-L. Huang, "Copy-Move Forgery Detection In Digital Image," In *Advances In Multimedia Information Processing-Pcm 2009*, Ed: Springer, 2009, Pp. 816-825.

[2] B. Mahdian And S. Saic, "Blind Methods For Detecting Image Fakery," *Ieee Aerospace And Electronic Systems Magazine,* Vol. 25, Pp. 18-24, 2010.

[3] B. Shivakumar And L. D. S. Santhosh Baboo, "Detecting Copy-Move Forgery In Digital Images: A Survey And Analysis Of Current Methods," *Global Journal Of Computer Science And Technology,* Vol. 10, 2010.

[4] K. N. Qureshi And A. H. Abdullah, "A Survey On Intelligent Transportation Systems," *Middle East Journal Of Scientific Research,* Vol. 15, 2013.

[5] W. Lu, W. Sun, J.-W. Huang, And H.-T. Lu, "Digital Image Forensics Using Statistical Features And Neural Network Classifier," In *Machine Learning And Cybernetics, 2008 International Conference On*, 2008, Pp. 2831-2834.

[6] S. Bayram, B. Sankur, N. Memon, And İ. Avcibaş, "Image Manipulation Detection," *Journal Of Electronic Imaging,* Vol. 15, Pp. 041102-041102-17, 2006.

[7] A. C. Popescu And H. Farid, "Exposing Digital Forgeries By Detecting Traces Of Resampling," *Signal Processing, Ieee Transactions On,* Vol. 53, Pp. 758-767, 2005.

[8] A. E. Dirik, S. Bayram, H. T. Sencar, And N. Memon, "New Features To Identify Computer Generated Images," In *Image Processing, 2007. Icip 2007. Ieee International Conference On*, 2007, Pp. Iv-433-Iv-436.

[9] M. Kharrazi, H. T. Sencar, And N. Memon, "Blind Source Camera Identification," In *Image Processing, 2004. Icip'04. 2004 International Conference On*, 2004, Pp. 709-712.

[10] M.-J. Tsai And G.-H. Wu, "Using Image Features To Identify Camera Sources," In *Acoustics, Speech And Signal Processing, 2006. Icassp 2006 Proceedings. 2006 Ieee International Conference On*, 2006, Pp. Ii-Ii.

[11] M.-J. Tsai And C.-S. Wang, "Adaptive Feature Selection For Digital Camera Source Identification," In *Circuits And Systems, 2008. Iscas 2008. Ieee International Symposium On*, 2008, Pp. 412-415.

[12] Y. Sutcu, S. Bayram, H. T. Sencar, And N. Memon, "Improvements On Sensor Noise Based Source Camera Identification," In *Multimedia And Expo, 2007 Ieee International Conference On*, 2007, Pp. 24-27.

[13] R. Bausvs And A. Kriukovas, "Digital Signature Approach For Image Authentication," *Electronics & Electrical Engineering,* 2008.

[14] T. Chen, J. Wang, And Y. Zhou, "Combined Digital Signature And Digital Watermark Scheme For Image Authentication," In *Info-Tech And Info-Net, 2001. Proceedings. Icii 2001-Beijing. 2001 International Conferences On*, 2001, Pp. 78-82.

[15] X. Zhou, X. Duan, And D. Wang, "A Semifragile Watermark Scheme For Image Authentication," In *Multimedia Modelling Conference, 2004. Proceedings. 10th International*, 2004, Pp. 374-377.

[16] M. Sridevi, C. Mala, And S. Sanyam, "Comparative Study Of Image Forgery And Copy-Move Techniques," In *Advances In Computer Science, Engineering & Applications*, Ed: Springer, 2012, Pp. 715-723.

[17] S. Rawat And B. Raman, "A Chaotic System Based Fragile Watermarking Scheme For Image Tamper Detection," *Aeu-International Journal Of Electronics And Communications,* Vol. 65, Pp. 840-847, 2011.

[18] M. Kirchner And R. Bohme, "Hiding Traces Of Resampling In Digital Images," *Information Forensics And Security, Ieee Transactions On,* Vol. 3, Pp. 582-592, 2008.

[19] H. Shah, P. Shinde, And J. Kukreja, "Retouching Detection And Steganalysis," *Ijeir,* Vol. 2, Pp. 487-490, 2013.

[20] R. Granty, T. Aditya, And S. Madhu, "Survey On Passive Methods Of Image Tampering Detection," In

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communication And Computational Intelligence (Incocci), 2010 International Conference On, 2010, Pp. 431-436.

[21] M. Sridevi, C. Mala, And S. Sandeep, "Copy–Move Image Forgery Detection In A Parallel Environment," 2012.

[22] W. Luo, J. Huang, And G. Qiu, "Robust Detection Of Region-Duplication Forgery In Digital Image," In *Pattern Recognition, 2006. Icpr 2006. 18th International Conference On*, 2006, Pp. 746-749.

[23] J. Wang, G. Liu, H. Li, Y. Dai, And Z. Wang, "Detection Of Image Region Duplication Forgery Using Model With Circle Block," In *Multimedia Information Networking And Security, 2009. Mines'09. International Conference On*, 2009, Pp. 25-29.

[24] N. D. Wandji, S. Xingming, And M. F. Kue, "Detection Of Copy-Move Forgery In Digital Images Based On Dct," *International Journal Of Computer Science Issues (Ijcsi),* Vol. 10, 2013.

[25] S. Bayram, H. T. Sencar, And N. Memon, "An Efficient And Robust Method For Detecting Copy-Move Forgery," In *Acoustics, Speech And Signal Processing, 2009. Icassp 2009. Ieee International Conference On*, 2009, Pp. 1053-1056.

[26] R. Davarzani, K. Yaghmaie, S. Mozaffari, And M. Tapak, "Copy-Move Forgery Detection Using Multiresolution Local Binary Patterns," *Forensic Science International,* Vol. 231, Pp. 61-72, 2013.

[27] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, And G. Bebis, "Image Forgery Detection Using Multi-Resolution Weber Local Descriptors," In *Eurocon, 2013 Ieee*, 2013, Pp. 1570-1577.

[28] H. Huang, W. Guo, And Y. Zhang, "Detection Of Copy-Move Forgery In Digital Images Using Sift Algorithm," In *Computational Intelligence And Industrial Application, 2008. Paciia'08. Pacific-Asia Workshop On*, 2008, Pp. 272-276.

[29] X. Bo, W. Junwen, L. Guangjie, And D. Yuewei, "Image Copy-Move Forgery Detection Based On Surf," In *Multimedia Information Networking And Security (Mines), 2010 International Conference On*, 2010, Pp. 889-892.

[30] B. Dybala, B. Jennings, And D. Letscher, "Detecting Filtered Cloning In Digital Images," In *Proceedings Of The 9th Workshop On Multimedia & Security*, 2007, Pp. 43-50.

[31] H. Farid, "Exposing Digital Forgeries In Scientific Images," In *Proceedings Of The 8th Workshop On Multimedia And Security*, 2006, Pp. 29-36.

[32] P. Kakar And N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *Information Forensics And Security, Ieee Transactions On,* Vol. 7, Pp. 1018-1028, 2012.

[33] G. Muhammad And M. S. Hossain, "Robust Copy-Move Image Forgery Detection Using Undecimated Wavelets And Zernike Moments," In *Proceedings Of The Third International Conference On Internet Multimedia Computing And Service*, 2011, Pp. 95-98.

[34] B. Mahdian And S. Saic, "Detection Of Copy–Move Forgery Using A Method Based On Blur Moment Invariants," *Forensic Science International,* Vol. 171, Pp. 180-189, 2007.

[35] J.-W. Wang, G.-J. Liu, Z. Zhang, Y. Dai, And Z. Wang, "Fast And Robust Forensics For Image Region-Duplication Forgery," *Acta Automatica Sinica,* Vol. 35, Pp. 1488-1495, 2009.

[36] Z. Mohamadian And A. A. Pouyan, "Detection Of Duplication Forgery In Digital Images In Uniform And Non-Uniform Regions," In *Uksim*, 2013, Pp. 455-460.

[37] A. C. Popescu And H. Farid, "Exposing Digital Forgeries In Color Filter Array Interpolated Images," *Signal Processing, Ieee Transactions On,* Vol. 53, Pp. 3948-3959, 2005.

[38] Z. Ting And W. Rang-Ding, "Copy-Move Forgery Detection Based On Svd In Digital Image," In *Image And Signal Processing, 2009. Cisp'09. 2nd International Congress On*, 2009, Pp. 1-5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[39] M. Bashar, K. Noda, N. Ohnishi, And K. Mori, "Exploring Duplicated Regions In Natural Images," *Ieee Transactions On Image Processing,*, P. 1, 2010.

[40] M. Sridevi, C. Mala, And S. Sandeep, "Copy–Move Image Forgery Detection," *Computer Science & Information Technology (Cs & It)*, Vol. 52, Pp. 19-29, 2012.

[41] A. J. Fridrich, B. D. Soukal, And A. J. Lukáš, "Detection Of Copy-Move Forgery In Digital Images," In *In Proceedings Of Digital Forensic Research Workshop*, 2003.

[42] M. Qiao, A. Sung, Q. Liu, And B. Ribeiro, "A Novel Approach For Detection Of Copy-Move Forgery," In *Advcomp 2011, The Fifth International Conference On Advanced Engineering Computing And Applications In Sciences*, 2011, Pp. 44-47.