A Survey on Block Based Copy Move Image Forgery Detection Techniques

Toqeer Mahmood[1], Tabassam Nawaz[2], Rehan Ashraf[1], Mohsin Shah[3], Zakir Khan[3], Aun Irtaza[4], Zahid Mehmood[1]

[1] Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan
Email: {toqeer.mahmood, rehan_ashraf94}@yahoo.com
[2] Department of Software Engineering, University of Engineering and Technology Taxila, Pakistan
Email: {tabassam.nawaz, zahid.mehmood}@uettaxila.edu.pk
[3] Department of Information Technology, Hazara University Mansehra, Pakistan
Email: {syedmohsinshah, zakirk2012}@gmail.com
[4] Department of Computer Science, University of Engineering and Technology Taxila, Pakistan
Email: aun.irtaza@uettaxila.edu.pk

Abstract — **In today's modern life, digital images have significant importance because they have become a leading source of information dissemination. However, the availability of image editing tools made it easier to forge the contents of a digital image; making the authenticity untrustful. Different techniques can be used to forge the digital images. Copy move forgery is the most popular and common approach where a specific part of an image is copied and pasted elsewhere in the same image to conceal unwanted part or object. In this study, we attempted to survey several passive block based copy move forgery detection techniques. A passive technique attempts to identify forgery in digital images without any prior information. A comparison between various techniques is also included.**

Keywords — Passive; Copy move; Forensics; Forgery; Authenticity; Digital image

I. INTRODUCTION

In today's modern life in which we are living, the digital images have significant importance because they have become a main source of information. An image broadcasted in TV news or in a newspaper usually assumed as a certificate of trust. It can also be presented as a proof for any incident in the court room. With the prevalent availablity of sophisticated image processing tools such as Adobe Photoshop, GIMP etc., a non-professional user can even change the contents of a digital image easily. Fig. 1 is showing the possible image forgery examples. Therefore, the contents authenticity of a digital image is a major concern. To deal with this issue digital image forensics has evolved as a new field of study.

Forging with the images is not a new problem, in fact many forgeries have been dispersed [1] uptill now since nineteenth century. According to Amsberry [2], only in US nearly 10% of all the published images were transformed digitally. In early 1840's Hippolyte Bayrad produced first forged image showing himself a vitim of suicide [3]. In 1860's after the US Civil War, an image of Abraham Lincoln was dispersed in which his head was superimposed onto the body of John Coalhoun [1]. In early 1990's, computers revolutionized the art with early great work by Hollywood such as Jurassic Park, Terminator and Forest Gump [3]. In 2001, after the incident of 9/11, several videotapes of Osama bin Laden dispersed. Many of them were, later on, proved to be forged when the forensics analysis is performed [4]. In 2008, Iran performed a test of rocketing of 3 missiles whereas an image of rocketing 4 missiles was circulated, which was later on proven to be fake [5,6]. Similarly, many more examples of forged images in 19th and 20th centuries can be found. As a result of preceding evidences in various application areas, the frequency of the forged images is growing rapidly. Consequently, digital technology began to erode the belief on digital images, so that apparently "seeing is no longer believing" [1,7]. All of these problems will get worse with the progress in computing industry and sophistication in the image editing tools [8]. This situation highlights the need for devising the techniques to verify the integrity of a digital image. The researchers interested in security of multimedia contents have suggested various methodologies that may be categorized into: a) active; and b) passive techniques, as shown in Fig. 2.

For authenticating the content of a digital image, digital watermarking [9-11] and digital signature [12, 13] have been proposed which are known as active techniques. However, these techniques require some pre-processing operations, like embedding watermark and signature when generating digital images, thus limiting their applications in practice [14].

In recent times, a new concept for authentication of digital image has emerged. It undertakes that the authentic image has some consistent inherent patterns introduced by the imaging devices and can only be altered after some manipulation operations. The authenticity of an image may be determined by identifying the source of a digital image or by detecting the patterns[15]. As compared to active techniques, this ideology do not require any pre-processing operations. Thus, it is categorized as passive or blind technique.

The remainder of the survey is presented as follows: the fundamental concepts of passive forensics are introduced in section II. In Section III, an overview of previous techniques in the area of block based copy move forgery detection are presented. Finally, the concluding remarks and challenges are given in Section IV.

978-1-5090-0436-2/15/$31.00 ©2015 IEEE

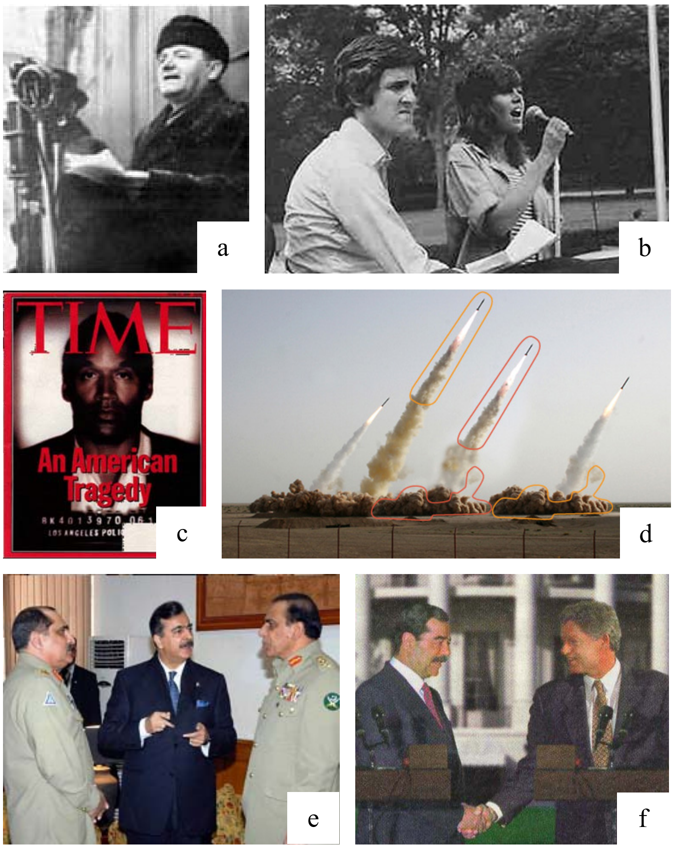

FIG. 1: EXAMPLES OF IMAGE FORGERIES REPORTED (A) THE PHOTOGRAPHER KAREL HAJEK AND VLADO CLEMENTIS ARE REMOVED [16], (B) COMPOSITE OF JANE FONDA AND JOHN KERRY [17], (C) TIME COVERS REPORTING ON THE CASE OF O.J. SIMPSON [15], (D) PHOTOMONTAGE OF IRAN MISSILE TEST [18], (E) FORMER PRIME MINISTER OF PAKISTAN YOUSAF RAZA GILANI [19], (F) PHOTOMONTAGE OF BILL CLINTON AND SADDAM HUSSAIN [20].

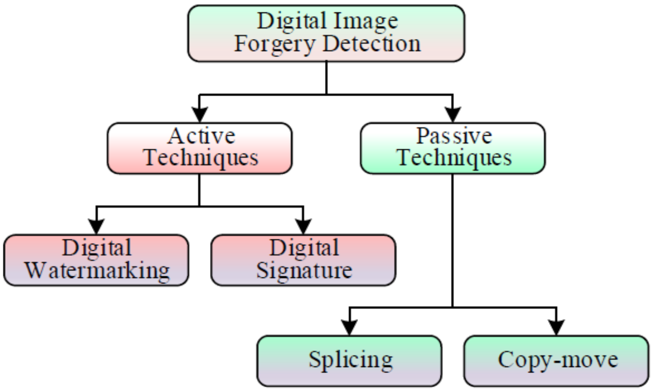

FIG 2. APPROACHES FOR AUTHENTICATION OF A DIGITAL IMAGE

II. FUNDAMENTAL CONCEPTS OF PASSIVE FORENSICS

This section of the paper describes briefly the principles of active and passive forensics, and shows the main difference between these techniques for digital image forensics.

A. Authentication based on Active Methods

The active methods may be categorized into two classes: the digital watermarking and the digital signature.

The digital watermarking is a two way process [21]. The source generates a watermark (*W*), encode it into an image (*I*) to get the watermark image (I_w). The receiver side scans the watermark image (I_w) and extracts the watermark (*W*) data to test whether the image has been altered [10, 22]. A digital watermark is a pattern of bits encoded into a digital image and scattered all around to avoid identification or modification. Thus, primarily the process of watermarking is to add secret data and recovering the same totally or partially for image authentication. However, this technique is unable to detect manipulations, performed before embedding the watermark.

In digital signature technique, the unique features of a digital image are extracted at the time of capturing [13, 23]. During authentication process, the same technique is applied to generate the signature again. The authenticity of the image may be identified through comparison.

As digital watermarking and digital signature has the same procedure and features, the disadvantages of both the techniques are also similar.

B. Authentication based on Passive Methods

The digital image authentication techniques based on passive methods are also known as digital image forensics or multimedia forensics. It is a process of validating visual contents of a digital image without any additional details aside from the image itself [24]. The passive methods may be categorized into two classes: the image source identification and forgery detection [15].

1) Image source identification

Different device can be used to a capture a digital image like cameras, scanners etc., which are accessible to an average consumer with ease. In a court room, if a digital image is presented as an evidence against an incident, identification of image acquisitioning device would be of main interest for determining the image integrity and authenticity. A solution to source device (camera) identification named EXIF (Exchangeable Image File) is being used in most digital cameras [25]. The cameras store some data such as manufacturer, model, image size, exposure time, JPEG quantization matrix [25], etc. as header in digital images. If this information is out of the range of the given camera, then the reported image is assumed as unauthentic.

2) Image forgery detection

Forging a digital image without any obvious traces is no longer difficult even for ordinary users with the help of Adobe Photoshop, GIMP etc. In general, image enhancement such as color or contrast adjustment is not considered a malicious forgery, because these do not change any contents of a real image. Therefore, adding, removing, modifying or retouching a scene or object in an image which would make the forgery hard to detect is a malicious forgery. Thus, image forgery detection can determine whether the image is authentic or forged to what extent. Image forgery detection techniques may further be categorized into two classes: splicing and copy move.

Image splicing is a method which deals with producing a forged image by copying and pasting a region from one or more images into another image [27]. In some cases human eye may be able to identify this kind of forgery because the spliced image may have inconsistencies in many features such as different lighting, color patterns, shadows [28] etc. Copy move is a most common image forgery technique for manipulating a semantics image [15]. A forger achieves copy move forgery by copying and pasting a part in the same image with the intent of hiding unwanted regions.

III. Block based Copy move Image Forgery Detection Techniques

Many techniques have been presented for block based copy move image forgery detection, following a typical procedure, as shown in Fig. 3. Due to the simplicity, copy move forgery is a common exercise of forging an image. The main objective is to classify the similar regions in copy move image forgery detection but the main issue is how to define "similar" [29]. A forger usually select textured regions from the image because they have matching color and noise variations. Furthermore, some post processing operation like blurring may have been applied by the forger along the corners of the forged regions which would make the detection harder by the naked eye.

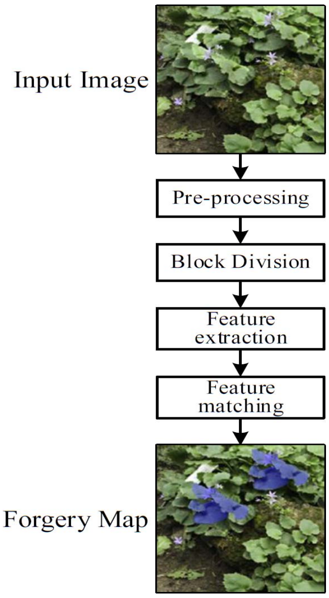

Fig. 3: Common Procedure of Copy Move Image Forgery Detection Techniques

At first stage in block based copy move forgery detection techniques, an image of size $M \times N$ may be pre-processed e.g. conversion from color to grayscale image. Then, the pre-processed image is subdivided into overlapping blocks of size $B \times B$ using equation 1:

$$\textit{Total blocks of an image} = (M - B + 1) \times (N - B + 1) \qquad (1)$$

From each of the extracted blocks, a unique representation as feature vectors is obtained. Then, for matching process these feature vectors may be arranged using sorting techniques such as lexicographic sorting, nearest neighbor etc. and some kind of distance measure is used between neighboring feature vectors such as Euclidean Distance. In verification step, the holes are filled and isolated blocks are removed using morphological operations and finally detection map is displayed.

In [20], initially the concept of passive copy move forgery detection was suggested. This concept was based on Discrete Cosine Transform (DCT) which uses DCT coefficients of the image blocks for matching. Lexicographical sorting is performed to reduce the computational cost and neighboring block pairs are considered to be possibly forged areas. As a similarity measure Euclidian distance is calculated among the two neighboring blocks. This technique assumes that the forged areas have not undergone any post processing operation and failed to detect small forged areas.

Later on, in [30], Principal Component Analysis (PCA) based technique is presented to reduce the length of feature vector with high discriminative power and reduced computational cost. Moreover, this technique showed robustness against Additive White Gaussian noise (AWGN), JPEG Compression with lower number of false positives. However, the accuracy rate is lower for small sized blocks and for JPEG quality level less than 50. Subsequently, an improved version of [30] is presented in [31] using blur invariants, PCA and kd-tree. PCA is used to obtain the reduced feature vector representation and kd-tree is adopted to identify the forged regions but the computation cost is high due to similarity threshold.

In [32], a technique using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) is presented. The authors obtained the low frequency coefficients using DWT and obtained the reduced feature vector representation by applying SVD on each sub-block of low frequency coefficients. The algorithm shown robustness and accuracy up to JPEG quality factor 70. In [33], a technique is suggested based on improved SVD but not robust against the image processing operations.

In [34], an algorithm based on DWT and log-polar coordinates is presented. To get the reduced dimension representation the authors applied DWT on the input image. The sub blocks of the image are mapped to log-polar coordinates. An exhaustive search method is applied and the phase correlation is used in block matching step. The algorithm showed lower computational time but the geometric operations are not discussed. Later on, in the work of [35], an algorithm is presented based on Log-Polar Fast Fourier Transform (LPFFT). This technique attempted to detect forged areas which are scaled and rotated. The FFT is a generalization of Discrete Fourier Transform with lower computational cost.

In [36], Fourier Mellin Transform (FMT) is used involving the log-polar mapping. To reduce the computational cost, bloom filters are used in the block matching process. This technique exhibited robustness with respect to compression, additive noise, scaling and rotation. However, this scheme addresses copied areas which are slightly scaled and rotated.

In [37], Zernike moments based algorithm is described that is invariant to different operations like JPEG compression, rotation, blurring and AWGN. The algorithm exhibited robustness against different degrees of rotation and high detection rate but not for the scaling. Later on, in [38], a similar approach is presented. The low approximation of the image is obtained through undecimated wavelet transform (UWT) and the Zernike moments are extracted from it. This approach has similar drawback as of [37].

In [39], an approach was presented using DWT and PCA aiming to improve the technique presented in [30]. DWT is applied on the image to reduce the size and obtained the low approximation coefficients. This technique is similar to [40] but the only difference is incorporation of PCA eigenvalue decomposition (PCA EVD). This technique does not perform well against compression and noise, especially for the small forged regions.

In [41], an improved form of [20] is suggested in which, DCT coefficients are obtained from each extracted block by applying DCT. These coefficients are then quantized by a factor “q” and rounded to the nearest integer. For getting feature factor, zigzag scan is perfumed and truncated the elements to only [p×B^2]. This technique is simple and straight forward with the power of detecting forged regions distorted by compression, blurring, and additive noise but does not address the scaling.

In [42], DCT method is presented again by exploiting the means of the DCT coefficients and circular blocks are used to extract the features $□=\{□_1, □_2, □_3, □_4\}$. The proposed technique not only reduced the feature length but showed robustness against detection of multiple copy move forgeries, noise and blurring as well. However, this method is not robust against compression, rotation and scaling.

In [43], exploited a novel algorithm using transform invariant features with respect to scaling, rotation, flipping, blurring, compressing and additive noise. The authors used MPEG-7 image signature tools for copy move forgery detection. The technique is quite difficult but minimize false positives by employing the procedure of multi-hypothesis matching.

In [44], circular blocks are extracted and rotation invariant uniform local binary patterns (LBP) are applied on the blocks for feature extraction. Gaussian filter is applied to an image and low frequency components are used that are more stable for forgery detection. This technique is robust to blurring, additive noise, rotation, flipping and compression. However, it is unable to detect forged regions rotated with arbitrary angles. In [45], the extracted blocks are filtered using the Wiener filter. Multiresolution LBP (MLBP) features are obtained from each of the block. The kd-tree is incorporated in matching step to reduce the computational cost and RANdom Sample Consensus (RANSAC) algorithm and to eliminate the false positives. This techniques showed the ability to detect the forged areas precisely against geometric distortions like scaling, rotation, compression, additive noise and blurring but failed to detect the forged areas with arbitrary rotated angles.

This section surveyed different techniques with their features, merits and demerits in the area of block based copy move forgery detection. A few of the above discussed techniques along with their characteristics are compared in Table 1.

TABLE 1. COMPARISON OF BLOCK BASED COPY MOVE IMAGE FORGERY DETECTION TECHNIQUES

Techniques	Feature Length	Rotation	Scaling	Compression	AWGN	Blurring	Complexity	Merits	Demerits
[20]	64	Y	Y	Y	N	N	O (64 K log K)	DCT signal energy concentrate on first few coefficients other negligible	Computational cost very high
[30]	32	N	N	Y	Y	N	O (32 K log K)	Feature vector dimension reduction, Robust against AWGN & JPEG Compression	Lower accuracy rate for small sized blocks and for low JPEG quality
[31]	72	N	N	Y	Y	Y	O (72 K log K)	Robust against AWGN & JPEG Compression (Q=70)	Computational cost high due to similarity threshold
[32]	8	N	N	Y	N	N	O (8 K log K)	Feature vector dimension reduction, lower computational cost than [20] and [30]	False positive still higher
[36]	45	Y	Y	Y	Y	Y	Execution time 2sec	Computational time decreased by incorporating bloom filters	Unable to detect when rotated with arbitrary angles and scale with larger factor
[37]	12	Y	N	Y	Y	Y	O (12 K)	Robust against AWGN, JPEG Compression, blurring & rotation (up to 30^o)	Scaling is not addressed
[41]	4	Y	N	Y	Y	Y	O (4 K log K)	Feature length reduced greatly, Robust to AWGN, JPEG Compression, blurring & rotation, lower computation cost than [20], [30] and [32]	Scaling is not addressed
[42]	4	N	N	N	Y	Y	O (4 K log K)	Feature length reduced greatly, ability to detect rotated regions, lower JPEG computation cost than [20], [30] and [32]	Rotation and scaling not addressed
[44]	18	Y	Y	N	Y	Y	O (18 K log K)	Robust to blurring, additive noise, rotation, flipping and JPEG compression	Unable to detect when rotated with arbitrary angles

I. Conclusion

As the copy move forgeries have taken commonplace in our daily lives, there is an increasing need of passive image forgery detection techniques to address various aspects of image forensics. Although several methods have been suggested in the field of copy move image forgery detection for particular cases but a method which give a generalized solution is still sought. This study presented a concise survey on various techniques dedicated to block based copy move forgery detection. This may help researcher's community to get new concepts and provide different solutions to the challenges in the field of block based copy move forgery detection. A comparison between some of the existing techniques is also presented in Table 1, which shows that each of the techniques have some kind of shortcomings. Thus, further research efforts are still required to address these shortcomings. Some of the major problems needing attention are to reduce the computational time, increase the accuracy, decrease the inaccuracy and the robustness against various geometric transformations. Furthermore, choosing an appropriate threshold is also a challenging task. Therefore, any future research endeavors may look into these issues and such algorithms are required to be developed that provide reliable solution with robust detection.

References

[1]. H. Farid, "Digital doctoring: how to tell the real from the fake," Significance, vol. 3, pp. 162-166, 2006.

[2]. C. Amsberry, "Alterations of photos raise host of legal, ethical issues," The Wall Street Journal, vol. 1, pp. 26-89, 1989.

[3]. T. Qazi, K. Hayat, S. U. Khan, S. A. Madani, I. A. Khan, J. Kołodziej, et al., "Survey on blind image forgery detection," IET Image Processing, vol. 7, pp. 660-670, 2013.

[4]. N. Krawetz, "A pictures worth digital image analysis and forensics," Black Hat Briefings, pp. 1-31, 2007.

[5]. M. Nizza and P. J. Lyons, "In an iranian image, a missile too many," The Lede, The New York Times News Blog, 2008.

[6]. S. Lian and Y. Zhang, "Multimedia forensics for detecting forgeries," in Handbook of Information and Communication Security, ed: Springer, 2010, pp. 809-828.

[7]. B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When seeing isn't believing [multimedia authentication technologies]," Signal Processing Magazine, IEEE, vol. 21, pp. 40-49, 2004.

[8]. A. Piva, "An overview on image forensics," ISRN Signal Processing, vol. 2013, 2013.

[9]. F. Y. Shih, Multimedia Security: Watermarking, Steganography, and Forensics: CRC Press, 2012.

[10]. C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," EURASIP Journal on Applied Signal Processing, vol. 6, pp. 613-621, 2002.

[11]. A. Khan, S. A. Malik, A. Ali, R. Chamlawi, M. Hussain, M. T. Mahmood, et al., "Intelligent reversible watermarking and authentication: Hiding depth map information for< i> 3D</i> cameras," Information Sciences, vol. 216, pp. 155-175, 2012.

[12]. C.-H. Tzeng and W.-H. Tsai, "A new technique for authentication of image/video for multimedia applications," in Proceedings of the 2001 workshop on Multimedia and security: new challenges, 2001, pp. 23-26.

[13]. C.-S. Lu and H.-Y. Liao, "Structural digital signature for image authentication: an incidental distortion resistant scheme," Multimedia, IEEE Transactions on, vol. 5, pp. 161-173, 2003.

[14]. M. P. Gomase and M. N. Wankhade, "Advanced Digital Image Forgery Detection: A Review," International Conference on Advances in Engineering & Technology (ICAET), pp. 80-83, 2014.

[15]. J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: a booklet for beginners," Multimedia Tools and Applications, vol. 51, pp. 133-162, 2011.

[16]. B. Mahdian and S. Saic, "Blind methods for detecting image fakery," IEEE Aerospace and Electronic Systems Magazine, vol. 25, pp. 18-24, 2010.

[17]. M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proceedings of the 7th workshop on Multimedia and security, 2005, pp. 1-10.

[18]. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," Information Forensics and Security, IEEE Transactions on, vol. 6, pp. 1099-1110, 2011.

[19]. http://www.fourandsix.com/photo-tampering-history/?currentPage=141.

[20]. 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.

[21]. F. Hartung and M. Kutter, "Multimedia watermarking techniques," Proceedings of the IEEE, vol. 87, pp. 1079-1107, 1999.

[22]. D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," Proceedings of the IEEE, vol. 87, pp. 1167-1180, 1999.

[23]. R. Bausvs and A. Kriukovas, "Digital Signature Approach for Image Authentication," Electronics & Electrical Engineering, 2008.

[24]. L. Zhou, D. Wang, Y. Guo, and J. Zhang, "Blur detection of digital forgery using mathematical morphology," in Agent and Multi-Agent Systems: Technologies and Applications, ed: Springer, 2007, pp. 990-998.

[25]. http://www.exif.org.

[26]. H. Farid, "Digital image ballistics from JPEG quantization," Technical Report TR2006-583, Department of Computer Science, Dartmouth College2006.

[27]. J. Dong, W. Wang, T. Tan, and Y. Q. Shi, "Run-length and edge statistics based approach for image splicing detection," in Digital Watermarking, ed: Springer, 2009, pp. 76-87.

[28]. Z. Fang, S. Wang, and X. Zhang, "Image splicing detection using color edge inconsistency," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 923-926.

[29]. Z. Zhang, Y. Ren, X.-J. Ping, Z.-Y. He, and S.-Z. Zhang, "A survey on passive-blind image forgery by doctor method detection," in Machine Learning and Cybernetics, 2008 International Conference on, 2008, pp. 3463-3467.

[30]. A. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image region [Technical Report]. 2004-515," Hanover, Department of Computer Science, Dartmouth College. USA, 2004.

[31]. 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.

[32]. G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750-1753.

[33]. L. Kang and X.-p. Cheng, "Copy-move forgery detection in digital image," in Image and Signal Processing (CISP), 2010 3rd International Congress on, 2010, pp. 2419-2421.

[34]. A. Myna, M. Venkateshmurthy, and C. Patil, "Detection of region duplication forgery in digital images using wavelets and log-polar mapping," in Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on, 2007, pp. 371-377.

[35]. Q. Wu, S. Wang, and X. Zhang, "Log-polar based scheme for revealing duplicated regions in digital images," Signal Processing Letters, IEEE, vol. 18, pp. 559-562, 2011.

[36]. 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.

[37]. S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Information Hiding, 2010, pp. 51-65.

[38]. 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.

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

[40]. M. Zimba and S. Xingming, "Fast and robust image cloning detection using block characteristics of DWT coefficients," JDCTA: International Journal of Digital Content Technology and its Applications, vol. 5, pp. 359-367, 2011.

[41]. Y. Huang, W. Lu, W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic science international, vol. 206, pp. 178-184, 2011.

[42]. Y. Cao, T. Gao, L. Fan, and Q. Yang, "A robust detection algorithm for copy-move forgery in digital images," Forensic science international, vol. 214, pp. 33-43, 2012.

[43]. 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.

[44]. L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, pp. 46-56, 2013.

[45]. 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.