International Journal of Inclusive Development
Citation IJID: **8**(01): 127-136, June 2022
DOI: 10.30954/2454-4132.1.2022.26
Peer-Reviewed Journal

A Review on Copy-move Forgery Detection

Henerita Khumallambam[1]*, Rajeev Rajkumar[2] and Durgamohon Polem[1]

[1]Research Scholar, [2]Department of Computer Science, MIT, Manipur, India

*Corresponding author: khhene@gmail.com

Received: 14 Mar., 2022 **Revised:** 29 May, 2022 **Accepted:** 03 June, 2022

Abstract

The digital images are becoming a concrete information source with the vast improvements in imaging technologies. So, it is necessary to maintain the originality and reliability of digital images which is challenging because of the advent of easy and extremely powerful and sophisticated digital image processing tools that can maliciously alter, manipulate and tamper digital images without leaving behind any noticeable sign. One of the effective way of identifying the manipulated image region known as copy-move forgery detection that recognizes the tampered region. It is performed by copying a region of the image and pasted on another region of the image in order to hide unwanted area of the image or replicate some area of the image. This paper, presents a review of various techniques of forgery detection in view of block based, keypoint based and hybrid based.

Keywords: Digital image, tamper, keypoint based, block based

INTRODUCTION TO DIGITAL IMAGES

Generally, Digital images were generated from digital scanner that scans records like photos, manuscripts, printed texts, etc. or from digital cameras (M.R. 2012). Today, in communication media images have become very useful. For the manipulation of images in earlier days, the images that were generated from traditional film cameras, professional information was required to perform such activities which was difficult for normal users. Nowadays, with the inexpensive devices, in these days the images are easy to acquire. The process of recording, storing and sharing of large number of images is possible by every person in the era of digital images, using the image processing techniques (Redi *et al.* 2011). And so Digital image tampering become a simple task.

DIGITAL IMAGE FORGERY

Digital image forgery differs from conventional image forgery by using digital images instead of a photograph (Birajdar and Mankar, 2013). Process of manipulating digital images for any purpose of crime is called digital image forgery. Due to the great development of image processing tools and also with the help of a powerful digital camera, manipulation of the image is becoming very easy which innovates to develop more automatic image forgery techniques in order to maintain the originality of the image. Some of the freely available image editing tool namely Adobe Photoshop, Coreldraw, GIMP and Corel paint shop makes this process of forgery more viable. Nowadays this

How to cite this article: Khumallambam, H., Rajkumar, R. and Polem, D. (2022). A Review on Copy-move Forgery Detection. *Int. J. of Inclusive Develop.*, **8**(01): 127-136.

Source of Support: None; **Conflict of Interest:** None

image forgery has been increased tremendously leading to an increase in crime activities. Forgery image can be created by hiding some significant or useful information or multiplying the objects present in the original image (Yerushalmy and Hel-Or, 2011). Image forgery can be categorized into two approaches namely passive and active approaches which are shown in Fig. 1.

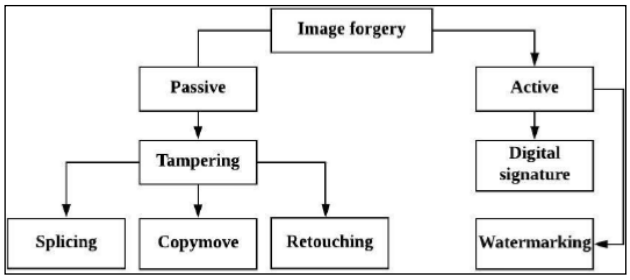

Fig. 1: Image Forgery Classification

1. Active/Intrusive/Non-Blind Approach

The two main active approach techniques are digital watermarking and digital signature in which data are embedded into the digital image at the time of the image generation. But in practice, this might limit their application. Here the information embedded cannot be extracted from the image rather tampered image can be easily detected (Cheddad *et al.* 2010).

Watermarking

One of the most popular techniques of active tampering detection is watermarking in which a security structure is embedded into the target image but most of the present imaging device does not have a watermarking or signature unit. The security structure is used for evaluating the integrity of the image and if any inconsistency is found with the structure, the image is assumed to be tampered. Usually, these watermarked images are made to made streams or to be invisible with the natural camera or scanner noise. There are also visible watermarking. A visually undetectable watermark is also existed that detects the change of single pixels and also identifies the location of the change that took place. Some built-in watermarking digital image generation mechanism also exist in which embedding watermark is not required at the time of image creation (Dadkhah *et al.* 2014).

Digital Signature

For detecting image forgery, the digital signature is also one of the kinds of the active method which is simple and forms a basic concept for authentication of the digital image. It is also defined as the authentication of digital documents by using a type of mathematical system. Usually, the digital signature is calculated by dividing the image into blocks of size 16 × 16 pixels of which N random matrices with entries are generated by using a secret key k that are consistently distributed in the interval [0,1]. For obtaining N random smooth patterns, a low pass filter is supplied on each of the random matrices repeatedly.

The system applies signing process for generation of a digital signature on the image. Image signing process contains following steps (Shivakumar *et al.* 2011):

(i) Decomposition of the image using parameterized wavelet feature.

(ii) Extraction of the Structural Digital Signature (SDS).

(iii) The extracted SDS is Cryptographically hashed to generate the image of the crypto signature by sender's private key.

(iv) The images delivered along with the crypto signature to the recipient.

The image and its corresponding digital signature are transmitted. The receiver then recomputed the signature of the received image. Then both the signatures are compared and if it matches, then it can be concluded that there is no tampering which means the received image is the original image.

As there is a need for some human intervention or a specialized camera, the active techniques have some limitations. Passive authentication technique is introduced in order to overcome this problem.

2. Passive/Non-Intrusive/Blind Approach

In image processing, one of the great challenges is passive image forensic. There is no specific tool for treating all the issues of passive approach, but there are many methods that can detect the image forgery in their own ways. Based on different statistics and semantics of the contents of the image, the passive approach usually deals with the analysis of the raw

image in order to detect the tampered image. In this type of approach, there is no need of embedding security construct in the image as like that of the active approach.

For this reason, it is also called as raw image analysis. Depending on the types of security construct used, there are several techniques or algorithm for detection or localizing the forgery in the image in passive approach. Regardless it aims for detecting of tampering on raw image. For measuring image authenticity or integrity, the passive approach uses the received image without any watermark or signature of the original image which is sent by the sender. The inconsistencies generated by tampering the image will disturb the underlying statistical properties which will be helpful in detection of forgery in the tampered image even though forgery image may not leave any visual evidence of having been tampered (B¨ohme and Kirchner, 2013).

Image Retouching: Image retouching is also known as a process of manipulating image which slightly changes the look of a subject which is shown in Fig. 2. It is considered to be less harmful compared to other image forgery techniques. The main purpose of image retouching is to enhance or change certain features of the original image but does not change significantly. It is mainly used by magazine photo editors for enhancing certain features of the image in order to make the image more attractive which are ethically wrong.

Fig. 2: Retouched Forgery Image

Image retouching is performed by detecting the blurring, enhancement, and changing illumination and color in the forged image. If the original image is available, then detection is easy but blink detection is a challenging task. Image retouching can be classified into global and local approach (Joseph and A.S. 2015). A global approach is usually performed by contrast enhancement and illumination whereas the local approach is performed in copy-move and splicing forgery.

Splicing: Image splicing is also one of the popular commonly used forgery technique in which the fake image is produced by using more than one image where copy-move uses only one image for creating a forgery which is shown in Fig. 3 (Salloum *et al.* 2018). In splicing forgery technique, higher order Fourier statistics are altered which provides in the detection process. Image splicing is considered to be a fundamental process which can also be done by crop and paste areas from same or different sources. There is a function available in digital tools like Photoshop which performs such technique of paste-up produced by binding together images. Even there are lots of news reporting cases which are involved in the usage of fake images.

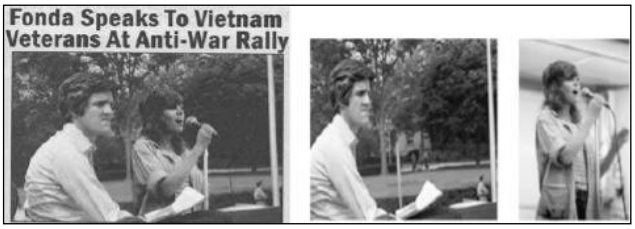

Fig. 3: Spliced Forgery Image

Usually, the spliced image shows edges, regions, and blur, lines at the place where splicing is performed. But due to the advent of new sophisticated editing tool, all these lines,edges, region, and blur are made to be a fuse inside the image which is not noticeable to the human eye and thus unable to detect the forgery. This becomes a challenging area for the researcher. Image splicing and steganography produce a tampered image which modifies the image smoothness, regularity, continuity, and periodicity but both have diverse approaches. Thus statistical approaches are usually used by both the steganalysis and the image splicing detection techniques. Normally dimensional feature vectors are used in image splicing techniques. The four common methods of steganalysis that are applied to image splicing detection (Moghaddasi *et al.* 2014) are 72-D, 78-D, 2-D Markov chain based, and method based on statistic moments extracted from the spatial domain and multi-block discrete cosine transform. The accuracy obtained by above mentioned methods are 73.78%, 75.83%, 76.25%, and 87.07% respectively.

Copy-move: The most popularly used manipulation technique is the copy-move image forgery in which some region of the image is copied and pasted to different regions in the same image. Post-processing operation like scaling, rotation, noise, translation, etc is also sometimes applied to the copied part and pasted it to some other area of the image. The dynamic range and color of the copied part are well-matched with the rest of the image as the copied part belongs to the same image. In order to make the fake part invisible to the human visualization, image related methods like scaling, noise, blur etc. are applied to the original image. Some of the methods are unable to distinguish like noise or color. Copy-move forgery is mainly performed either to produce identical region or to camouflage some region in the image (Muhammad *et al.* 2012).

COPY-MOVE DIGITAL IMAGE FORGERY DETECTION

The most popular type of image forgery is a copy-move forgery as it can be done very easily with any photo editing tools. In this type of technique, both the copied and pasted part are from the same image thus the tampered region will have the same statistical properties like color temperature, illumination conditions and noise with the image which is invisible to the naked eyes. Usually, the altered region is mainly substituted by fabric, foliage, grass etc. (Anand *et al.* 2014) which are easy to fuse with the image contents that have similar color and textures. The correlation generated between the original image and a tampered region can be used for detecting copy-move forgery. The tampered region may not be similar with the original image because of the forgery produced may be saved using lossy JPEG format and also may use any localized processing tools. Thus, we can develop the requirements for the detection algorithm (Lin *et al.* 2009) which follows as:

(i) The algorithm should be able to perceive small image segments approximately.

(ii) The detection algorithm should work in less computational time with reduced false positive match.

(iii) The forged region should be connected component instead of a collection of the small region or separate pixels.

Usually, preprocessing operation is possible in many of the copy-move forgery detection (CMFD) methods. Generally, images are first converted into grayscale images by merging the color channel together. Copy-move forgery detection can be categorized into the block based approach and keypoint based approach for extracting feature vector. In blocked based approach, the image is divided into equal-sized blocks and feature vectors are calculated for each block. Detection is carried out by finding the match block which has similar feature vector. But in the case of the keypoint approach, instead of dividing block, keypoint is identified by marking the region with high entropy. Similar feature vectors are identified by matching these keypoints (Li *et al.* 2015).

1. Block based Copy-move Image Forgery Detection

Normally, CMFD performs an exhaustive search for finding the matched feature vector which is a time consuming process. Dividing the whole image into blocks will help in reducing the time consumption to some extent. This type of CMFD comes under block-based approach in which the image is divided into smaller overlapping or nonoverlapping blocks. For each block, the feature is extracted which will be used in matching the similar blocks which indicate the presence of forgery in the image. Block based approach are invariant to different image post-processing operation like noise, blur, compression etc. but variant to the rotation and scaling operation.

2. Key-point based Digital Image Forgery Detection

The main drawback of block based approach is overcome by keypoint based forgery detection in which keypoint based approach is invariant to scaling and rotation. In this type of method, keypoints are identified by marking the area with high entropy in the image and then for each keypoint, feature vectors are extracted. The feature vectors are then sorted lexicographically and stored in a matrix. Forgery in the image is detected by selecting the keypoints which are very close to each other in the sorted matrix. The main drawback of this keypoint based approach is that it cannot detect forgery in a at surface on the image. The two most commonly used keypoint methods can be named

as a scale invariant feature transform (SIFT) and speeded up robust features (SURF).

LITERATURE SURVEY ON IMAGE FORGERY DETECTION

INTRODUCTION

Digital images are the most influential and broadly used as regular for communication which has a major influence on our culture and can perform a significant part in our everyday life. The availability of handling and low-cost processes makes accepting digital image as official document in business and additional fields. The rise in technological advancement enables us to feature or take away vital capabilities from an image, such that it is problematic to detect hints of tampering. The use of some of the worldly experienced and knowledged manipulating and altering digital images makes easy and causes digital forgeries with the used of editing softwares such as, Photoshop, 3D Max, CorelDraw, etc. Because of the increasing number of crime activities and forgeries digital image forgery detection has currently established significant attention, especially during the past few years.

During last decades, many researchers have developed many techniques for doctored image detection and this topic become a hot research area in image processing and information security community. CMF is one the commonest methods in image forgery.

All the CMF detection techniques implemented in the past decades are based on either key points or block matching. This section presents a brief review on the classification of CMF detection techniques.

1. Block based Techniques

Yanjun *et al.* (2012) presents a novel technique for CMF detection using overlapping fixed-size block division and low frequency DCT coefficients. To reduce the computational complexity, the coefficient matrix is represented by a circular block and the circular block is divided into four parts where a feature is extracted from each part. In Jie and Guo (2013), SVD is used to reduce the dimensionality of the block feature extracted using 2D-DCT. In Kumar *et al.* (2014), PCA is used to reduce the dimension of the feature. In Bovik and Liu (2001) (Bovik and Liu, 2001), to measure the block difference, HVS is used. In Sunil *et al.* (2013), an adaptive threshold is developed which makes the detection system less false matching. Ashima *et al.* (2013) also proposes a system using DCT.

Yanging *et al.* (2011) proposes an improved DCT based system for CMF detection in which the feature vectors are lexicographically sorted resulting into a sorted list of neighbouring duplicated image blocks. An improved lexicographical sorting algorithm is presented in Jie *et al.* (2011) for CMF detection.

Mehdi *et al.* (2011) (Ghorbani *et al.* 2011) uses DWT and DCT-QCD for CMF detection.

Zhouchen *et al.* (2009) examines the hidden double quantization effect of DCT coefficients for CMF detection. Detection of fine-grained, fast computation time, the ability to work with partial decompressing of the JPEG images and not affected by different tempering methods are some advantages of the system.

Leida *et al.* (2014) proposes a CMF detection system using circular pattern matching and Polar Harmonic Transform.

Image noises like Photo Response Non-Uniformity and sensor pattern noise are introduced to images while capturing. Giovanni *et al.* (2014) uses these noises and a Markov random field for CMF detection.

Babak and Saic (2010) proposes a CMF detection method using blur moment invariants. The system is robust to image attacks due to blur, noise, JPEG compression and changes in contrast.

Reza *et al.* (2013) uses multiresolution local binary patterns and k-d tree for CMF detection where k-d tree is used to reduce the computational time. Additionally, RANSAC algorithm is used to reduce the false matching.

Weimin *et al.* (2010) proposes an angle estimator using the peak frequencies during interpolation that exists in the image edge map spectrum and the rotation angle. Different geometrical operations such as zooming, rotation and combination of both can be predicted from the type of peaks.

Yuenan (2013) proposes a CMF detection system using approximate nearest neighbor searching and polar cosine transform. A novel locality-sensitive hashing algorithm is developed to achieve the

nearest neighbor searching and to remove the false matching a post-verification technique is applied.

Guangjie *et al.* (2011) uses the Hu moment and the circle block for CMF detection. A lower feature dimension is generated for better time complexity.

Gavin *et al.* (2013) proposes an expanding block algorithm for CMF detection which can successfully identify the duplicated region's shape and size. The system is immune to small change in illumination, JPEG compression or Gaussian blur.

Adam and Sorel (2018) develops a JPEG-based constraint for CMF detection system that reduces the missed matching and this constraint can be applied to most of the existing CMF detection system.

Chien-Chang *et al.* (2017) proposes a CMF detection system using seven invariant moment features.

Junliu *et al.* (2017) uses an overlapping circular block to divide the input image where Discrete Radial Harmonic Fourier Moment features are extracted from each circular block. 2-nearest neighbor is applied to search the similar blocks. In Leida *et al.* (2013), local binary pattern is used as circular block feature which is rotation invariant. In Toqeer *et al.* (2017), local binary pattern variance of the stationary wavelets is used as the feature. In Wang *et al.* (2009), the circular blocks are divided into four concentric circles and the mean of each circle is taken as the feature.

An improved block-based system is proposed in Yuecong *et al.* (2017), where the first column of a feature matrix is the sum of the feature vectors of each block and are sorted according to the sum of feature vectors. A threshold is used to mark the dissimilarities between the blocks.

In Al-Qershi and Khoo (2016), k-means clustering is used to group the similar blocks and Zernike moments is used for block matching.

Hsieh and Wu (2006) proposes a Multi-Rings Zernike Transform (MRZT) for tempering detection which is geometric transformation invariant.

SPT and LBP is used in Muhammad *et al.* (2013) to detect CMF in YCbCr color space. LBP histograms of multi-oriented and multi-scale subbands obtained from Cb and Cr by applying SPT transform are used to define the texture information of the image.

Fridrich *et al.* (2003) investigates the various issues in CMF detection and proposed an efficient technique using auto-correlation which successfully detects the doctored part even under different image post processing attacks.

Popescu and Farid (2005) describes various resampling signals like up-sampled, interpolate and down-sampled in order to trace the signals in the input image for forgery part of the image.

Luo *et al.* (2006) proposes a CMF detection algorithm using seven features from color space. The first three features are calculated from the red, green and blue frequencies and the rest four features are calculated from the Y frequency by dividing the block in two halves in four different ways.

Langille and Gong (2006) proposes a CMF detection system using K-dimensional tree and Zero-Normalized Cross Correlation (ZNCC). K-d tree is used to group the similar patterns and ZNCC is for matching.

Yang and Huang (2009) uses the singular values as the feature for block matching which is robust to JPEG compression. Ting and Wang (2009) also took the advantages of singular values in their proposed system.

Zhang and Su (2008) proposes a CMF detection approach using Discrete Wavelet Transform (DWT) and phase correlation. A similar model for forgery detection is also given in Saiga and Kulkarni (2010).

Lin *et al.* (2009) proposes a method that uses radix sort to sort the extracted feature vectors. Detection of forgery is performed by marking large accumulated number which is evaluated from the shift vector calculated from the sorted list. To obtain the final result, the connected component analysis and median filtering are done.

Chaitawittanum (2012) proposes a CMF detection system using block color information and Hausdorff Distance where Hausdroff Distance is applied to cluster the similar color blocks.

Sridevi *et al.* (2012) proposes a method that divide overlapping blocks and lexicographical sorting in a parallel manner in order to decrease the computational time of detection. As an alternative to lexicographical sorting, a counting bloom filter is used in Bayram *et al.* (2009).

Bin *et al.* (2013) proposes a system using DWT and fast Walsh-Hadamard Transform (FWHT) for feature extraction. Multi-hop jump (MHJ) algorithm is used to jump over some "unnecessary testing blocks" (UTB) for efficiently matching of feature block. In Preeti and Rathore (2012), DWT and Lexicographic sorting are used.

Seniha and Ulutas (2013) proposes a system using two dimensional Fourier Transform (2D-FT). The system is able to detect multiple forgery.

A rotation and reflection invariant feature descriptor generated from block pixel information is used as feature in Solorio and Nandi (2009). Correlation coeffcient is then calculated to measure the similarity between blocks.

Jen-Chun *et al.* (2015) proposes a CMF detection system using histogram of orientated gradients (HOG) as block feature and lexicographical sorting to get the similar block pairs.

2. Key-point based Techniques

Xunyu and Lyu (2010) describes a novel and robust CMF detection system using SIFT key-points. Best-bin-first algorithm and affine transform are used to match the keypoints and reduce the false matching respectively. In Irene *et al.* (2013), J-Linkage algorithm is used to cluster the key-points. In Irene *et al.* (2011), SIFT feature is used and more over the system tries to recover the geometric transformation performed during cloning.

In Bin *et al.* (2018), an improved SIFT feature extractor is used for CMF detection. Guonian and Wan (2017) proposes an optimized J-Linkage algorithm using the concept of clusters and affine transformation. Another method using SIFT and bicoherence features is given by Zhang *et al.* (2014).

Chihaoui *et al.* (2014) proposes a system using SIFT and SVD.

Pandey *et al.* (2014) combines the advantages of SURF and SIFT for CMF detection.

Liu *et al.* (2014) proposes a method using an improved SIFT by combining BFSN clustering and color filter array (CFA) features. The system is able to detect multiple forgeries.

Sudhakar *et al.* (2014) presents a novel algorithm using SIFT and Chan-Vese's Level Set where Chan-Vese's Level Set is used to reduce the key-points.

Fan *et al.* (2017) proposes a hybrid local feature extractor using KAZE and SIFT to produce more number of key-points.

Seung-Jin *et al.* (2010) proposes a CMF detection system using Zernike moments which utilizes the advantage of rotation invariant. A similar model is proposed in Zahra (2012) where the system can detect at area.

Bilgehan *et al.* (2013) proposes a novel local feature called Krawtchouk moments for CMF detection.

Maryam *et al.* (2014) proposes a detection scheme using Mirror-reection Invariant Feature Transform (MIFT) local feature and a redfined affine transform.

Shen *et al.* (2016) proposes a novel technique using ORB features and orientated FAST key-points in each of Gaussian scale space. Random sample consensus (RANSAC) algorithm is used to reduce the false matching.

Thirunavukkarasu *et al.* (2018) introduces a robust technique using discrete stationary wavelet transform along with multi dimension scaling for CMF detection.

Xiang-Yang (2017) proposes a CMF detection system by dividing the input image into nonoverlapping and irregular superpixels and from each superpixels key-points are detected using improved SURF algorithm.

Davide *et al.* (2015) proposes a Dense-field techniques for CMF detection. A PatchMatch algorithm is used for finding the similar points in the image.

Lowe (2004) uses fast nearest-neighbor and Hough transform to recognize objects and verification is done by Least-squares solution.

Jung and Lacroix (2001) uses a variant of Harris detector to find the interest points which is robust to outliers.

Flusser *et al.* (1995) uses image moments which are calculated from the blurred images acquired by a linear shift-invariant imaging system.

Ewerton *et al.* (2015) presents a novel technique using multi-scale analysis and voting processes which is robust to scale and rotation.

Li *et al.* (2015) proposes a scheme that divided the image into semantically independent patches which is used to detect patch matching. The matching process consists of two stages. An affine transform

and an Expectation-Maximization algorithm are used to define the forged region.

CONCLUSION

The main intention of copy-move forgery is to replicate some part of the image or to hide some content in the image. In this paper, we discussed the various digital image forgery mainly focussing on copy-move forgery and a brief review on different copy-move forgery detection algorithms. Some recent works in block based and keypoint based approached for detection of copy move forgery detection is presented.

REFERENCES

Al-Qershi, O.M. and Khoo, B.E. 2013. "Copy-move forgery detection using on locality sensitive hashing and k-means clustering," *in Information Science and Applications (ICISA) 2016* (K.J. Kim and N. Joukov, eds.), (Singapore), pp. 663–672, Springer Singapore.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Tongo, L.D. and Serra, G. 2013. "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," *Signal Processing: Image Communication*, **28**(6): 659 – 669.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D. and Serra, G. 2011. A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, **6**: 1099-1110.

Anand, V., Hashmi, M.F. and Keskar, A.G. 2014. "A copy move forgery detection to over- come sustained attacks using dyadic wavelet transform and SIFT methods," in *Intelligent Information and Database Systems* (N. T. Nguyen, B. Attachoo, B. Trawin´ski, and K. Somboonviwat, eds.), (Cham), pp. 530–542, Springer International Publishing.

Bayram, S., Sencar, H.T. and Memon, N. 2009. "An efficient and robust method for detecting copy-move forgery," in 2009 *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1053–1056.

Bin, Y., Xingming, S., Xianyi, C., Zhang, J. and Xu, L. 2013. "An efficient forensic method for copy–move forgery detection based on DWT-FWHT.," *Radio Engineering*, **22**(4).

Birajdar, G.K. and Mankar, V.H. 2013. "Digital image forgery detection using passive techniques: A survey," *Digital Investigation*, **10**(3): 226 – 245.

Bovik, A.C. and Liu, S. 2001. "DCT-domain blind measurement of blocking artifacts in DCT-coded images," in 2001 *IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings* (Cat. No.01CH37221), **3**: 1725–1728.

Bravo-Solorio, S. and Nandi, A.K. 2009. "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling," in *17th European Signal Processing Conference*, pp. 824–828.

B¨ohme, R. and Kirchner, M. 2013. *Counter-Forensics*: Attacking Image Forensics, New York, NY: Springer New York, pp. 327-366.

Cao, Y., Gao, T., Fan, L. and Yang, Q. 2012. "A robust detection algorithm for copy-move forgery in digital images," *Forensic Science International*, **214**(1): 33 – 43.

Chaitawittanun, N. 2013. "Detection of copy-move forgery by clustering technique," *International Proceedings of Computer Science & Information Technology*, **50**(6).

Cheddad, A., Condell, J., Curran, K. and Kevitt, P.M. 2010. "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, **90**(3): 727– 752.

Chen, C.-C., Wang, H. and Lin, C.-S. 2017. "An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection," *Multimedia Tools and Applications*, **76**: 26503–26522.

Chierchia, G., Poggi, G., Sansone, C. and Verdoliva, L. 2014. "A bayesian-MRF approach for PRNU-based image forgery detection," *IEEE Transactions on Information Forensics and Security*, **9**: 554–567.

Chihaoui, T., Bourouis, S. and Hamrouni, K. 2014. "Copy-move image forgery detection based on SIFT descriptors and SVD-matching," in *International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pp. 125–129.

Cozzolino, D., Poggi, G. and Verdoliva, L. 2015. "Efficient dense-field copy-move forgery detection," *IEEE Transactions on Information Forensics and Security*, **10**: 2284–2297.

Dadkhah, S., Manaf, A.A., Hori, Y., Hassanien, A.E. and Sadeghi, S. 2014. "An effective SVD-based image tampering detection and self-recovery using active watermarking," *Signal Processing: Image Communication*, **29**(10): 1197 -1210.

Davarzani, R., Yaghmaie, K., Mozaffari, S. and Tapak, M. 2013. "Copy-move forgery detection using multiresolution local binary patterns," *Forensic Science International*, **231**(1): 61 – 72.

Flusser, J., Suk, T. and Saic, S. 1995. "Image features invariant with respect to blur," *Pattern Recognition*, **28**(11): 1723 – 1732.

Fridrich, A.J., Soukal, B.D. and Luk, A.J. 2003. "Detection of copy-move forgery in digital images," in *Proceedings of Digital Forensic Research Workshop*.

Ghorbani, M., Firouzmand, M. and Faraahi, A. 2011. "DWT-DCT (QCD) based copy-move image forgery detection," in 2011 *18th International Conference on Systems, Signals and Image Processing*, pp. 1–4.

Gupta, A., Saxena, N. and Vasistha, S. 2013. "Detecting copy move forgery using DCT," *International Journal of Scientific and Research Publications*, **3**(5).

Hsieh, C.-T., Wu, Y.-K. and Hung, K.-M. 2016. "Geometric invariant semi-fragile image watermarking using real symmetric matrix," *WSEAS Transaction on Signal Processing*, **2**: 612–618.

Hu, J., Zhang, H., Gao, Q. and Huang, H. 2011. "An improved lexicographical sort algorithm of copy-move forgery detection," in *Second International Conference on Networking and Distributed Computing (ICNDC)*, pp. 23–27.

Huang, Y., Lu, W., Sun, W. and Long, D. 2011. "Improved dct-based detection of copy-move forgery in images," *Forensic Science International*, **206**(1): 178 – 184.

Jaberi, M., Bebis, G., Hussain, M. and Muhammad, G. 2014. "Accurate and robust localization of duplicated region in copy–move image forgery," *Machine Vision and Applications*, **25**: 451–475.

Jin, G. and Wan, X. 2017. "An improved method for sift-based copy-move forgery detection using non-maximum value suppression and optimized J-Linkage," *Signal Processing: Image Communication*, **57**: 113 – 125.

Joseph, R.M. and A.S. C. 2015. "Survey on image manipulation detection," *International Research Journal of Engineering and Technology*, **2**(4): 740–744.

Jung, I.-K. and Lacroix, S. 2001. "A robust interest points matching algorithm," in Proceedings Eighth IEEE *International Conference on Computer Vision. ICCV* 2001, **2**: 538–543.

Ketenci, S. and Ulutas, G. 2013. "Copy-move forgery detection in images via 2D-Fourier Transform," in *International Conference on Telecommunications and Signal Processing (TSP)*, pp. 813–816.

Khan, S. and Kulkarni, A. 2010. "Reduced time complexity for detection of copy-move forgery using discrete wavelet transform," *International Journal of Computer Applications*, **6**(7): 31–36.

Kumar, S., Desai, J. and Mukherjee, S. 2013. "A fast DCT based method for copy move forgery detection," in 2013 *IEEE Second International Conference on Image Information Processing (ICIIP-2013*), pp. 649–654.

Lai, Y., Huang, T., Lin, J. and Lu, H. 2018. "An improved block-based matching algorithm of copy-move forgery detection," *Multimedia Tools and Applications*, **77**: 15093–15110.

Langille, A. and Gong, M. 2006. "An efficient match-based duplication detection algorithm," in *the 3rd Canadian Conference on Computer and Robot Vision (CRV'06)*, pp. 1–8.

Lee, J.-C., Chang, C.-P. and Chen, W.-K. 2015. "Detection of copy-move image forgery using histogram of orientated gradients," *Information Sciences*, **321**: 250 – 262.

Li, J., Li, X., Yang, B. and Sun, X. 2015. "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, **10**: 507–518.

Li, L., Li, S., Zhu, H., Chu, S.-C., Roddick, J.F. and Pan, J.-S. 2013. "An efficient scheme for detecting copy-move forged images by local binary patterns," *Journal of Information Hiding and Multimedia Signal Processing*, **4**(1): 46–56.

Li, L., Li, S., Zhu, H. and Wu, X. 2014. "Detecting copy-move forgery under affine transforms for image forensics," *Computers & Electrical Engineering*, **40**(6): 1951 – 1962.

Li, Y. 2012. "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," *Forensic Science International*, **224**(1): 59 – 67.

Lin, H.-J., Wang, C.-W. and Kao, Y.-T. 2009. "Fast copy-move forgery detection," WSEAS *Transactions on Signal Processing*, **5**(5): 188–197.

Lin, Z., He, J., Tang, X. and Tang, C.-K. 2009. "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition*, **42**(11): 2492 – 2501.

Liu, G., Wang, J., Lian, S. and Wang, Z. 2011. "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, **34**(5): 1557 – 1565.

Liu, L., Ni, R., Zhao, Y. and Li, S. 2014. "Improved SIFT-based copy-move detection using BFSN clustering and CFA features," in 2014 *Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 626–629.

Lowe, D.G. 2004. "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, **60**: 91–110.

Luo, W., Huang, J. and Qiu, G. 2006. "Robust detection of region-duplication forgery in digital image," in *Proceedings of the 18th International Conference on Pattern Recognition* - Vol. 04, ICPR '06, (Washington, DC, USA), pp. 746–749, IEEE Computer Society.

Lynch, G., Shih, F.Y. and Liao, H.-Y. M. 2013. "An efficient expanding block algorithm for image copy-move forgery detection," *Information Sciences*, **239**: 253 – 265.

M.R. 2012. "Application of computer vision technique on sorting and grading of fruits and vegetables," *Journal of Food Processing & Technology*, **3**(8).

Mahdian, B. and Saic, S. 2010. "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication*, **25**(6): 389 – 399.

Mahmood, T., Irtaza, A., Mehmood, Z. and Mahmood, M.T. 2017. "Copy-move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images," *Forensic Science International*, **279**: 8 – 21.

Mamolu, M.B., Uluta, G. and Uluta, M. 2013. "Detection of copy-move forgery using krawtchouk moment," in *International Conference on Electrical and Electronics Engineering (ELECO)*, pp. 311–314.

Moghaddasi, Z., Jalab, H.A. and Noor, R.M. 2014. "SVD-based image splicing detection," in *International Conference on Information Technology and Multimedia*, pp. 27–30.

Muhammad, G., Al-Hammadi, M.H., Hussain, M. and Bebis, G. 2014. "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, **25**: 985–995.

Muhammad, G., Hussain, M. and Bebis, G. 2012. "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation*, **9**(1): 49 – 57.

Novozmsk, A. and Orel, M. 2018. "Detection of copy-move image modification using JPEG compression model," *Forensic Science International*, **283**: 47 – 57.

Pan, X. and Lyu, S. 2010. "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, **5**: 857–867.

Pandey, R.C., Singh, S.K., Shukla, K.K. and Agrawal, R. 2014. "Fast and robust passive copy-move forgery detection using SURF and SIFT image features," *in International Conference on Industrial and Information Systems (ICIIS),* pp. 1–6.

Popescu, A.C. and Farid, H. 2005. "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, **53**: 758–767.

Redi, J.A., Taktak, W. and Dugelay, J.-L. 2011. "Digital image forensics: a booklet for beginners," *Multimedia Tools and Applications*, **51**(133–162).

Ryu, S.-J., Lee, M.-J. and Lee, H.-K. 2010. "Detection of copy-rotate-move forgery using zernike moments," in *Information Hiding* (R. B¨ohme, P. W. L. Fong, and R. Safavi-Naini, eds.), (Berlin, Heidelberg), pp. 51–65, Springer Berlin Heidelberg.

Salloum, R., Ren, Y. and J. Kuo, C.-C. 2018. "Image splicing localization using a multitask fully convolutional network (MFCN)," *Journal of Visual Communication and Image Representation*, **51**: 201 – 209.

Shivakumar, B.L., Dr, L. and Baboo, S.S. 2011. "Detection of region duplication forgery in digital images using SURF," in *International Journal of Computer Science* Issues.

Silva, E., Carvalho, T., Ferreira, A. and Rocha, A. 2015. "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *Journal of Visual Communication and Image Representation*, **29**: 16 – 32.

Sridevi, M., Mala, C., Sandeep, S. and Meghanathan, N. 2012. "Copy–move image forgery detection in a parallel environment," *SIPM, FCST, ITCA, WSE, ACSIT, CS and IT*, **6**: 19–29.

Sudhakar, K., Sandeep, V.M. and Kulkarni, S. 2014. "Speeding-up SIFT based copy move forgery detection using level set approach," in 2014 *International Conference on Advances in Electronics Computers and Communications*, pp. 1–6.

Sunil, K., Jagan, D. and Shaktidev, M. 2014. DCT-PCA based method for copy-move forgery detection," in *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol II* (S.C. Satapathy, P.S. Avadhani, S.K. Udgata, and S. Lakshminarayana, eds.), (Cham), pp. 577-583, Springer International Publishing.

Thirunavukkarasu, V., Satheesh Kumar, J., Chae, G.S. and Kishorkumar, J. 2018. "Non- intrusive forensic detection method using DSWT with reduced feature set for copy-move image tampering," *Wireless Personal Communications*, **98**: 3039– 3057.

Wang, J., Liu, G., Li, H., Dai, Y. and Wang, Z. 2009. "Detection of image region duplication forgery using model with circle block," in 2009 *International Conference on Multimedia Information Networking and Security*, **1**: 25–29.

Wang, X.-Y., Li, S., Liu, Y.-N., Niu, Y., Yang, H.-Y. and Zhou, Z.-L. 2017. "A new keypoint- based copy-move forgery detection for small smooth regions," *Multimedia Tools and Applications*, **76**: 23353–23382.

Wei, W., Wang, S., Zhang, X. and Tang, Z. 2010. "Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery," *IEEE Transactions on Information Forensics and Security,* **5**: 507–517.

Yadav, P. and Rathore, Y. 2012. "Detection of copy-move forgery of images using discrete wavelet transform," *International Journal on Computer Science and Engineering*, **4**(4): 565–570.

Yang, B., Sun, X., Guo, H., Xia, Z. and Chen, X. 2018. "A copy-move forgery detection method based on CMFD-SIFT," *Multimedia Tools and Applications*, **77**: 837–855.

Yang, F., Li, J., Lu, W. and Weng, J. 2017. "Copy-move forgery detection based on hybrid features," *Engineering Applications of Artificial Intelligence,* **59**: 73 – 83.

Yang, Q.-C. and Huang, C.-L. 2009. "Copy-move forgery detection in digital image," in *Advances in Multimedia Information Processing - PCM* 2009 (P. Muneesawang, F. Wu, Kumazawa, A. Roeksabutr, M. Liao, and X. Tang, eds.), (Berlin, Heidelberg), pp. 816–825, Springer Berlin Heidelberg.

Yerushalmy, I. and Hel-Or, H. 2011. "Digital image forgery detection based on lens and sensor aberration," *International Journal of Computer Vision*, **92**: 71–91.

Zahra, M. 2012. "Image duplication forgery detection using two robust features," *Research Journal of Recent Sciences,* **1**(12): 1–6.

Zhang, J., Feng, Z. and Su, Y. 2008. "A new approach for detecting copy-move forgery in digital images," in *Communication Systems*, 2008. ICCS 2008. *11th IEEE Singapore International Conference on,* pp. 362–366, IEEE.

Zhang, J., Ruan, Q. and Jin, Y. 2014. "Combined SIFT and bi-coherence features to detect image forgery," in 2014 *12th International Conference on Signal Processing (ICSP),* pp. 1859–1863.

Zhang, T. and Wang, R. 2009. "Copy-move forgery detection based on SVD in digital image," in 2009 *2nd International Congress on Image and Signal Processing*, pp. 1– 5.

Zhao, J. and Guo, J. 2013. "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International,* **233**(1): 158– 166.

Zhong, J., Gan, Y., Young, J., Huang, L. and Lin, P. 2017. "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools and Applications*, **76**: 14887–14903.

Zhu, Y., Shen, X. and Chen, H. 2016. "Copy-move forgery detection based on scaled ORB," *Multimedia Tools and Applications*, **75**: 3221–3233.