International Journal of Future Generation Communication and Networking
Vol. 11, No. 2 (2018), pp.11-22
http://dx.doi.org/10.14257/ijfgcn.2018.11.2.02

Image Copy Move Forgery Detection: A Review

Saba Mushtaq[1]* and Ajaz Hussain Mir[2]

[1,2]*Department of Electronics and Communication Engineering,*
National Institute of Technology Srinagar India 190006
[1]*sab.mushtaq@gmail.com,* [2]*ahmir@rediffmail.com*

Abstract

Technological development in digital world has led to a huge increase in the popularity of digital images in all domains of life. However, sophisticated and easy to use photo editing software tools have made manipulation of images very easy. Thus there is a need to authenticate images especially in legal matters. The field of image authentication and forgery detection has gained huge popularity lately. A key domain in this regard is copy-move forgery detection. Copy move forgery involves copying a portion of an image and pasting it to a different location in same image, with a purpose to conceal facts. In this paper we attempt to review recent developments in the field of copy move detection. This paper dwells on the detection of copy move forgery based on block based and key point methods, and give a detailed comparison of the state of art techniques.

Keywords: *Copy-move Forgery, Region Duplication Detection, Forgery detection, Image Forensics*

1. Introduction

Advances in imaging technology have increased many folds and has led to the development of high-resolution digital cameras and powerful computers resulting in digital multimedia content becoming ubiquitous throughout society [1]. Moreover, easy understandability of image content as compared to text makes them more suitable for communication [2]. All this has led to many governmental, legal, scientific, and news media organizations to rely on digital multimedia content to make critical decisions, convey information and use as evidence of specific events. However huge dependence on digital media content has proved to be problematic either because of the tremendous development of photo editing software tools. Easy availability of these software packages has made image forgery incredibly easy [3]. According to the Wall Street Journal, 10% of all color photographs published in United States were actually digitally altered and retouched [4]. The scientific community has also been subject to forgeries [5]. Proverb like 'seeing is believing' is not relevant in today's life. There is a huge question mark over the use of digital images as evidences in court rooms and for other sensitive matters. Thus authenticating genuineness of images has become mandatory and as such image authentication has become a widely researched area [6,7,8]. Digital image forensics is the field that has evolved to establish integrity and authenticity of digital images and the driving force behind this field is image forgery. Though there are, perhaps, an uncountable number of ways to manipulate and tamper with digital images however copy-move is the most common image tampering technique, which involves copying a portion of image and pasting it somewhere else in the same image to conceal or multiply a part of the image to change the information conveyed by it. In literature copy-move forgery detection is one of most widely researched area. A number of review papers are available in the field of blind forgery detection [6,7,8,13]. However, this paper entirely focuses on

Received (January 5, 2018), Review Result (March 1, 2018), Accepted (March 2, 2018)

ISSN: 2233-7857 IJFGCN

the copy move forgery detection process and also presents the comparison of the available methods.

The remainder of the paper is organized as: Section 2 describes the overview of Image authentication and introduces copy-move forgery. In Section 3 general framework of copy move detection techniques is given. These techniques are further divided into block-based and key point-based approaches. Section 4 presents the available datasets for copy-move forgery detection. In Section 5 gives a comparison of the state of art techniques and conclusion is drawn in Section 6.

2. Image Authentication

Existing methods for image authentication can be broadly classified into two categories active authentication and passive authentication [7].

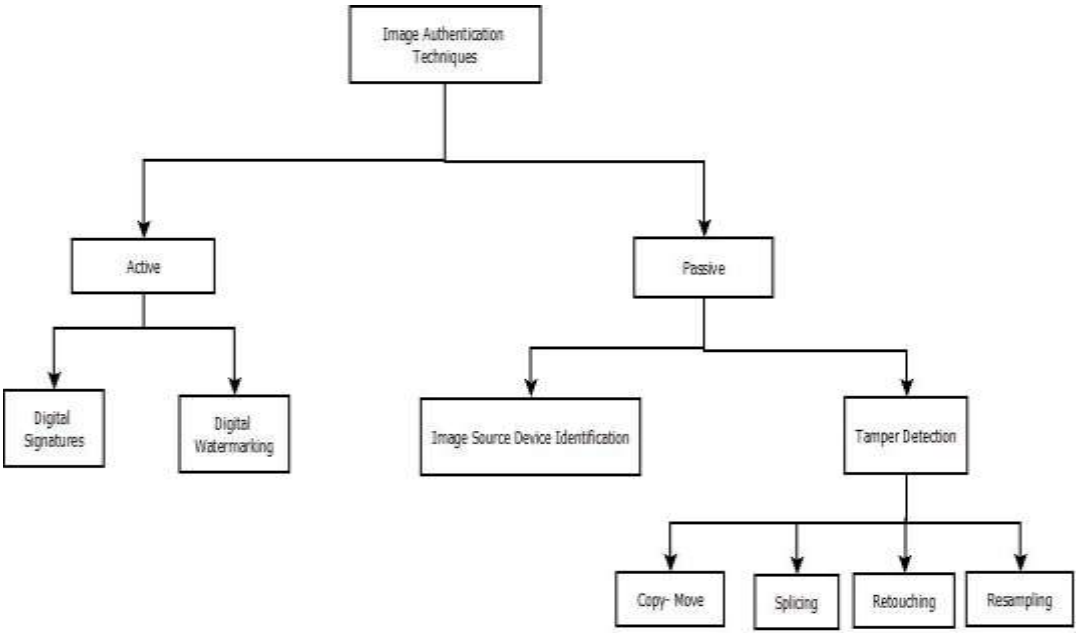

Figure 1. Image Authentication Techniques [7]

Active authentication include watermarking and digital signatures [9,10] and Passive authentication techniques are classified as source device identification and tamper detection [11]. Active authentication requires the availability of original image for the insertion of digital signature or water mark at the time of generation of image; however passive authentication overcomes this requirement as it requires no prior knowledge about the image and thus gaining enormous attention. For this reason they are also called as passive or blind techniques. This drawback of active image authentication limits this approach to special imaging equipment. In Passive authentication, the first category i.e., Source device identification is based on detecting camera fingerprints, which are the traces that are left by the image acquisition steps and the storage phases [6]. The second category i.e. tamper-detection techniques addresses the issue of the changes that are brought into the image by the process of editing. While there are ways to prevent identification of source such as removing pattern noise, adding noise of another camera to image but these require the forger to master the professional knowledge and are beyond the scope of average user. However, tampering image is a more general case and within the scope of a layman credit to the available easy to use photo editing software. Thus we focus on the tamper detection techniques. There are a number of ways to tamper image like splicing, copy-move, retouching and enhancement [7]. However, splicing and copy-

move are the two most common techniques that entirely change the message conveyed by the image [6]. While splicing involves merging of two images, copy move is copying a portion of an image and pasting it to different location in same image. Since color, dynamic range, texture and statistical attributes of the pasted region is same as original image copy-move detection becomes a complex problem[14]. Next section gives the detailed account of copy-move detection.

3. Detection of Copy Move Forgery

An example of copy- move forgery is shown in Figure 2. Figure shows an original image and its forged counterpart.

Figure 2. Left is the Original Image, Right is the Tampered Image

Copy move forgery detection techniques can be broadly classified into three types [8] one is the block based detection, second the key-point based detection and third brute force detection.

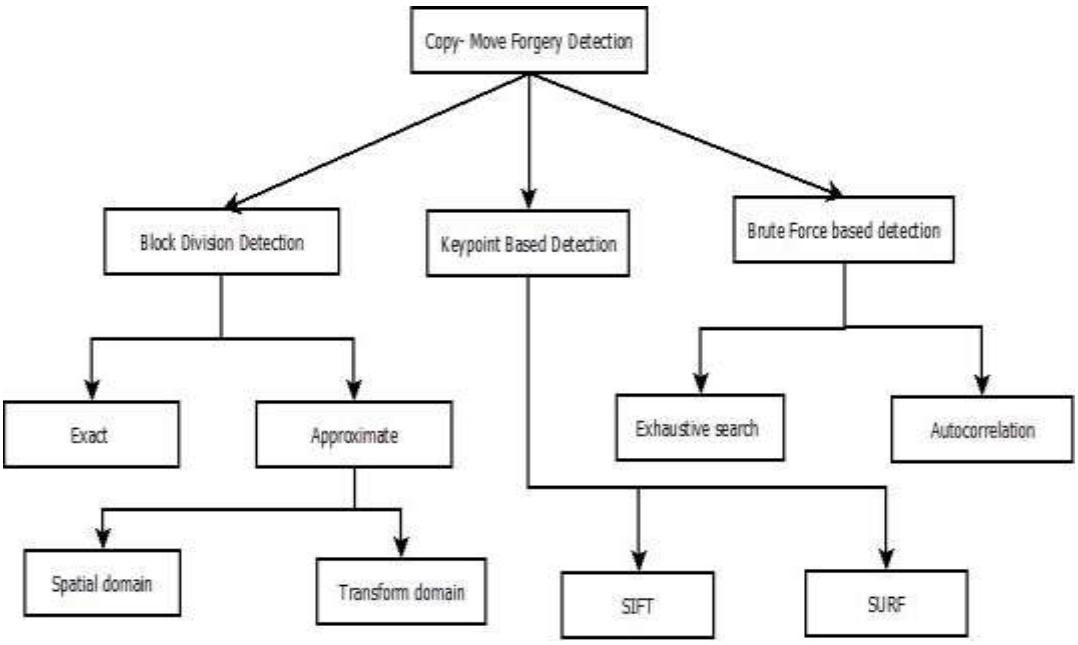

Figure 3. Copy Move Forgery Detection Techniques

The simplest solution to the problem of copy-move forgery is brute force detection which involves comparison of image to every shifted version of itself [8]. The problem with this method is its computational complexity. Autocorrelation method is an improvement over exhaustive search technique. However, it can be applied only when large image patches have been copy-pasted [12].

The key point based method depends on extraction of important key points like corners, edges, blobs in the image while block based approach relies on dividing image into blocks either overlapping or non-overlapping and features are extracted from each block and compared against each other[8]. Lot of research work is carried out in these two categories detailed in next section.

3.1 Block based Approaches

Block based techniques give better results than exhaustive search and autocorrelation techniques. The forged image is split into blocks of equal size. Theses blocks may be either be over lapping blocks or non-overlapping blocks. A general frame work for block based copy move forgery detection is shown below in Figure 4.

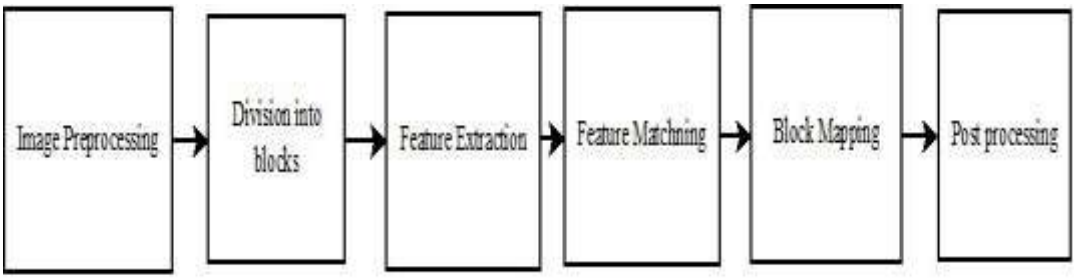

Figure 4. General Framework in Block Based Copy-Move Detection

The first step of preprocessing is optional. This step includes enhancement of image for a given feature extraction method and to contain unwanted data [14]. Conversion of image into gray scale is the most commonly used preprocessing operation [13-17]. In this step most images are converted to gray scale using I= .228R+ .587G+ .114 B to merge the RGB channels. YCbCr color system can be used interchangeably to operate on luminance or chrominance components [18]. The conversion of image to different color plane reduces dimensionality of the data and improves visual appearance of image. This in turn means reduction in computational complexity and improvement in processing speed.

Next step is division of image into blocks either overlapping or non over lapping. The block division method improves the computation complexity for matching process in copy-move detection over exhaustive search method. The block division is followed by feature extraction of the blocks. Techniques like Discrete cosine transform, Principal component analysis, DyWT, DWT [19-23], gray values[24] have been used for feature extraction. Techniques which reduce computation complexity and improve speed and robustness are preferred. Feature extraction is followed by feature matching for locating the copy pasted regions. Forged areas are defined by the extracted features. Sorting[15,16,20,22] ,Correlation[25],Euclidean distance[17] calculation have been used for the purpose of matching.

The last step post processing includes the isolation of the matched blocks to locate copy-pasted regions. This step either removes the matched block from image, mask the matched blocks or colors the image as black other than the copy-pasted regions. The most important step is the feature extraction step. Features are extracted from each block and are compared to find a match. The result can be an exact match or approximate one. The features extracted for blocks are in the form of frequency, texture, polar transforms and dimension reduction [26]. Feature extraction techniques are given in Table 1 below:

Table 1. Summary of Feature Extraction Techniques

Feature extraction technique	Papers
Frequency Transforms	Fridrich et al. [12], Popescu[19], Cao et al.[21], Huang et al[20], Muhammad et al.[17], Myna et al.[135], Zhang et al.[25], Zhao and Guo[27],
Texture	Lynch et al.[24], Lee [28], Luo et al.[29], Langille and Gong[31], Ardizzone et al. [15], Bravo-Solorio and Nandi [30].
Moment invariant	Mahdian and saic[32].
Log polar transforms	Bayram et al.[23]

a) Frequency Transforms

Frequency transform is most popular and one of the earliest techniques used for block based methods. Among the initial attempts Fridrich et al gave a method which is based on discrete cosine transform, DCT [12]. Exhaustive search method was used by Fridrich which was followed by block matching technique based on DCT. DCT has the advantage that most energy is concentrated on first few coefficients while other coefficients are very small. This technique is robust against retouching operation but gives no account of robustness against other techniques like jpeg compression.

Popescu proposed a technique that replaces the feature extraction technique DCT by principal component analysis (PCA)[19] in Fridrich's method. Feature vector representing each block form a matrix and covariance matrix is calculated for the same, followed by eigen value calculations. These eigenvalues signify the matrix and are considered to be robust against noise and compression but resampling and rotation change the eigenvalues. This method is considered to be efficient as features used are half that were used by Fridrich.

Muhammad *et al.*, [17] proposed a copy-move forgery detection method based on dyadic wavelet transform (DyWT). DyWT being shift invarient is more suitable than DWT. Image is decomposed into approximate and detail subbands which are futher divided into overlapping blocks and the similarity between blocks is calculated. Based on high similarity and dissimilarity pairs are sorted. Using thresholding matched pairs are obtained from the sorted list.

Haung *et al.*, [20] proposed a scheme based on DCT features. In this method the feature vector is reduced by truncating high frequency of coefficients which results in better performance than Popescu's method [19] in terms of robustness against rotation and in terms of speed in comparision to fridrich's method[12]. Robustness against JPEG compression with different quality factors, Gaussian blurring and additive white Gaussian noise are also demonstrated. However, this method is highly sensitive only when the copy-pasted areas are not too small. Cao *et al.*, [16] proposed a technique which is also based on DCT. However, this technique is based on DCT of circular blocks instead of square blocks. Because of circular block representation the complexity is reduced and the technique is capable of detecting multiple copy-move forgeries in an image. The drawback with this technique is that its effectiveness is demonstrated against post processing operations only like blurring and noise addition while there is no mention of rotation, scaling operations. Zhao and Guo[27] presented a technique which applies Singular Value decomposition (SVD) to the blocks after the DCT quantization. SVD extracts only a single largest value which reduces dimensionality of features. This technique is robust against Gaussian blurring, AWGN, JPEG compression and their mixed operation however this technique is also not tested for preprocessing forgery techniques. Zhang *et al.*, [25] presented a method that uses low frequency sub bands from

DWT exhibiting low computational complexity but with a drawback of dependability of speed on location of copy-pasted region.

Bashar *et al.*, [33] developed a technique that detects duplication using two robust features based on DWT and kernel principal component analysis (KPCA). KPCA-based projected vectors and multi resolution wavelet coefficients subsequent to image-blocks are arranged in the form of a matrix on which lexicographic sorting has been carried out. Translation Flip and translation Rotation are also identified using global geometric transformation and the labeling technique to detect the forgery. This method eliminates the off-set frequency threshold which otherwise is to be manually adjusted as in other detection methods.

b) Texture & Intensity Based Methods.

Texture exists in natural scenes and image properties such as smoothness, coarseness, regularity represent texture content [15]. Thus it can be used to locate similarity in forged images created by copy move forgery. Langille and Gong[31] proposed use of k-dimensional tree which uses a method that searches for blocks with similar intensity patterns using matching techniques. Use of kd-tree reduces the computational complexity.

Lynch *et al.*, [24] developed expanding block algorithm for duplicate region detection. In this method image is divided into overlapping blocks of size SxS. For each block grey value is calculated to be its dominant feature. Based on the comparison of this dominant factor a connection matrix is created. If the connection matrix has a row of zeros, then the block corresponding to this row is not connected to any other block in the bucket. This way duplicate regions are detected. This method is good at identifying the location and shape of the forged regions and direct block comparison can be done without sacrifice in performance time.

Luo *et al.*, [29] proposed an algorithm to extract image features using the statistical analysis of pixels of small overlapped blocks of an image, then they compare the similarity of these blocks. Finally, possible duplicated regions are identified using intensity- based characteristic features. It is efficient and robust against various post-processing operations, such as lossy compression, noise contamination, blurring and a combination of these operations, resulting in an accuracy of 96% and a false negative of 9% in the case of mixed operations. The drawback of this approach is that it is sensitive to small variations between duplicate regions due to noise and lossy compression.

Typically, RGB, illumination, spatial color and gray values are the basic components in representing the color information. These components are extracted through the color space, color quantification and similarity measurement. The color information is invariant with respect to scaling, translation and rotation as proposed by Bravo-Solorio and Nandi [30].

Meanwhile, Ardizzone *et al.*, [15] introduced the bit plane analysis to classify gray scale texture in the image content. However, the bit plane analysis is weak in detecting JPEG images due to the modification of intensity value in JPEG compression not been persistent.

c) Moment Invariant

Moment invariant is a set of features that are invariant to translation, rotation and scaling. The moments invariant was initially employed in copy-move by Mahdian and Saic [32] using blur invariant moment. The blur moment that represented by the function of central moments is resilient to blur degradation, additive noise and arbitrary contrast changes. However, extracting this feature from a large image will increase the computational complexity. This complexity can be reduced with a combination of blur moment and DWT [34].

d) Dimension Reduction

Dimension reduction techniques are commonly used with domain features to reduce the dimensionality of the image and improve the complexity. These techniques are Singular Value Decomposition (SVD) and Locally Linear Embedding (LLE). The SVD is generally stable, scales, and achieves rotation invariance for both algebraic and geometric properties. SVD reduces computational complexity and is robust to various operations particularly rotation, scaling, Gaussian noise and filtering [35]. However, SVD results in loss of image details resulting in the low performance in JPEG compression.

Alternatively, LLE can be implement to reduce dimensionality in high-dimensional dataset Zhao[27]. SVD has a higher overall performance of robustness to various operations and computational complexity.

e) Other Methods

Hong Shao *et al.*, [36] proposed a phase correlation method based on polar expansion and adaptive band limitation. Fourier transform of the polar expansion on overlapping windows pair is calculated and an adaptive band limitation procedure is applied to obtain a correlation matrix where peak is effectively enhanced. After estimating the rotation angle of the forgery region, a searching algorithm in the sense of seed filling is executed to display the whole duplicated region. This approach can detect duplicated region with high accuracy and robustness to rotation, illumination adjustment, and blur and JPEG compression.

Copy-move detection proposed by Sekeh [37] offers improved time complexity by using sequential block clustering. Clustering results in reduced search space in block matching and improves time complexity as it eliminates several block-comparing operations. When number of cluster is greater than threshold, local block matching is more efficient than lexicographically sorting algorithm.

3.2 Key-point based Approaches

The key-point features extract the distinctive local features such as corners, blobs, and edge from the image [8]. Each feature is presented with a set of descriptor produced within a region around the features. The descriptor helps to increase the reliability of the features to the affine transformation. Then, both features and descriptors in the image are classified and matched to each other to find the duplicated regions in the copy-move forgery [26].

Scale invariant feature transform (SIFT) [38,39,47] and Speed up robust features (SURF) [40-42] features have been widely used to extract key points in image. Recently Harris corner detectors have also been employed for key point extraction [43-45]. SIFT techniques are highly robust against post processing and intermediate operations[47] however they are computationally complex and incapable to determine forgeries in area which are flat due to lack of reliable key points[46]. SURF features where proposed to improve the performance of SIFT. Bo *et al.*, [40] proposed that SURF reduce the false acceptance rate considerably that too for high resolution images but lacks in detection if the copy pasted area is very small. Mishra *et al.*, [42] later demonstrated that though SURF features improve speed but they reduce accuracy. Harris corner detector extracts edges and corners from a region. Harris corners were proposed to improve performance of SIFT based methods. Kakar and Sudha [43] proposed a technique that combined Laplacian of Gaussian (LOG) with Haris filters. This technique exhibited robustness against scaling and rotation. Recently Yu *et al.*, [45] proposed to use non maximal suppression technique to obtain evenly and roughly distributed points. This technique increased the running time than SIFT and SURF feature based techniques.

Based on the above review, both block based method and key point method have their pros and cons. The advantage with the block based method is that they give the exact

extent and shapes of the copied areas while key point based methods only give the location of key points on the copy pasted regions. Moreover, if the forged area exhibits certain structure it may be entirely missed by key point based method [32].

4. Publically Available Datasets

To benchmark the performance of available copy-move detection techniques it is necessary that all techniques are tested on a common datasets. Moreover, these datasets should provide a wide range of images including natural images with realistic forgeries carried out on them. Presently the available datasets are listed below in Table 2.

Table 2. Publically Available Datasets

Database	Number of Images	Image Size
Columbia University[48]	1845	128x128
CASIA V 1.0[49]	1725	374x256
CASIA V 2.0[49]	12614	240x160 to 900x600
CoMoFoD[50]	260	512x512
MICC F2000[46]	2000	2048x1536
MICC F600[46]	600	800x533 to 3888x259

5. Comparison

This Paper presented the state of art method available for copy-move detection. A brief summary of the techniques based on block division are given in Table 3 and key point based detection methods are summarized in Table 4. below with their strengths and limitations.

Table 3. Block based Copy-move Detection Techniques

Paper	Technique Used	Sorting technique Used	Advantaged	Limitations	Performance
Fridrich et al.[12]	DCT of overlapping block	Lexicographical sorting	Avoids selection of isolated segments	High computation complexity	-
Popescu & Farid [19]	PCA of overlapping block	Lexicographical sorting	Reduced feature set	Not robust against rotation	50% for small block size 100% for 16x16 block size
Muhammad et al [17]	Dyadic wavelet transform(DyWT)	High similarity and dissimilarity	DyWT is shift invariant thus robust to rotation	Not tested for all post processing operations	Accuracy= 95.9 %
Haung et al. [20]	Truncating high frequency of DCT coefficients	Lexicographical sorting	Reduced feature vector	Not robust to geometric transformation	Accuracy= 90%
Cao et al. [16]	DCT of circular blocks	Lexicographical sorting	Able to detect multiple duplicate regions	Not tested for preprocessing operations	Accuracy= 80%

Zhao and Guo[27]	DCT with SVD	Lexicographical sorting	Detect and localize multiple regions	Not robust to geometric transformation	Accuracy= 96.1 %
Zhang et al. [25]	LL of DWT	-	Low computation complexity	Speed depends on position of the copy pasted region	-
Bashar et al. [33]	DWT and KPCA of overlapping blocks	Lexicographical sorting	Robust against rotation, translation and flipping	Not robust to scaling	Accuracy = 96%
Langille and Gong[31]	intensity patterns of blocks	Kd-sorting	Removes isolated mis-matches	Not tested for post processing operations.	-
Lynch et al. [24]	Enhanced expanding block algorithm	-	Effective in localizing size and shape of forgeries	Not robust to rotation and translation	Accuracy= 73%
Luo et al.[29]	Statistical analysis of pixels of overlapping blocks	Lexicographical sorting	Robust against post processing operations	Not robust against noise and compression S	Accuracy= 96%
Bravo-Solorio and Nandi [30].	Log Polar coordinates	-	Robust to rotation , scaling and translation	Tested for post processing operations only	TPR=.17 TNR=.98
Ardizzone et al. [15]	Texture descriptors	Lexicographical sorting	Robust to JPEG compression	Not robust against geometric transformations	Precision =95%

Table 4. Key-point based Detection Methods

Paper	**Technique Used**	**Advantaged**	**Limitations**
Amerini et al. [46]	SIFT	Robust against geometric transformation	Forged regions are not localized
Ardizzone et al.[47]	SIFT	High stability for both intermediate and post processing operations	Not tested for jpeg compression
Bo et al [40]	SURF	Reduce false matches and robust to transformations	Miss forged areas if size is small
Mishra et al [42]	SURF	Improve processing time.	Reduce accuracy
Kakar and Sudha [43]	Features extracted from Laplacian of Gaussian (LoG) combined with Harris filter.	Robust against scaling and rotation	Similar objects can be falsely considered forged

6. Conclusion

Copy-move forgery has become one of the most common and easy to carry techniques to manipulate images. This paper has presented a detailed review of available copy-move forgery detection techniques. From the literature review we concluded that there are a few challenges which are still open and need to be addressed. First of all is the issue of a common benchmark. The challenge of lack of a common benchmark limits the comparability and reproducibility of presently available algorithms. Though a number of datasets are available but still there is a need to develop datasets for observing the impact of geometric transformation on images and the techniques used to create copy-move forged images. Furthermore, the available techniques have not been evaluated on the basis of a common performance metrics which could have eased the comparison of the techniques. Robustness of algorithms is also an issue. Robustness to various post processing operation like blurring, sharpening, jpeg compression that are carried out for copy-move cannot be handled by any particular algorithm alone.

References

[1] https://en.wikipedia.org/wiki/Scientific_Working_Group_%E2%80%93_Imaging_Technology.
[2] G. Liu, J. Wang, S. Lian and Z. Wang, "A passive image authentication scheme for detecting region-duplication forgery with rotation", Journal of Network and Computer Applications, vol. 34, no. 5, **(2011)**, pp. 1557-1565.
[3] S. F. Chang, "Blind passive media forensics: motivation and opportunity", Multimedia Content Analysis and Mining, **(2007)**, pp. 57-59.
[4] C. Amsberry, "Alterations of photos raise host of legal, ethical issues", Wall Street J, **(1989)** January.
[5] H. Farid, "Exposing digital forgeries in scientific images", Proc. ACM multimedia and security workshop, **(2006a)**, pp. 29-36.
[6] O. M. Al-Qershi and B. E. Khoo, "Passive detection of copy-move forgery in digital images: State-of-the-art", Forensic science international, vol. 231, no. 1, **(2013)**, pp. 284-295.
[7] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey", International Journal of Advanced Science and Technology, vol. 73, **(2014)**, pp. 15-32.
[8] S. Bayram, H. T. Sencar and N. Memon, "A survey of copy-move forgery detection techniques", In IEEE Western New York Image Processing Workshop, IEEE, **(2008)** September, pp. 538-542.
[9] S. Katzenbeisser and F. Petitcolas, "Information hiding techniques for steganography and digital watermarking", Artech house, **(2000)**.
[10] I. J. Cox, M. L. Miller, J. A. Bloom and C. Honsinger, "Digital watermarking", San Francisco: Morgan Kaufmann, vol. 1558607145, **(2002)**.
[11] W. Zeng, H. Yu and C. Y. Lin, (Eds.), "Multimedia security technologies for digital rights management", **(2006)**, pp. 383-412.
[12] 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)**.
[13] V. Christlein, C. Riess, J. Jordan, C. Riess and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches", IEEE Transactions on information forensics and security, vol. 7, no. 6, **(2012)**, pp. 1841-1854.
[14] O. Miljkovi, "Image Pre-Processing Tool", Kragujev. J. Math., vol. 32, **(2009)**, pp. 97-107.
[15] E. Ardizzone, A. Bruno and G. Mazzola, "Copy-move forgery detection via texture description", In Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, ACM, **(2010)** October, pp. 59-64.
[16] Y. Cao, T. Gao, L. Fan and Q. Yang, "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images", Forensic Sci. Int., vol. 214, **(2012)**, pp. 33-43.
[17] G. Muhammad, M. Hussain and G. Bebis, "Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform", Digit, Investig., vol. 9, **(2012)**, pp. 49-57.
[18] Q. Wu, S. Wang and X. Zhang, "Detection of image region-duplication with rotation and scaling tolerance", Second International Conference, ICCCI, **(2010)**, pp. 100-108.
[19] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Department Computer Science, Dartmouth College, Technology Report TR2004-515, **(2004)**.
[20] Y. Huang, W. Lu, W. Sun and D. Long, "Improved DCT-based Detection of Copy-Move Forgery in Images", Forensic Sci. Int., vol. 206, **(2011)**, pp. 178-184.
[21] Y. Cao, T. Gao, L. Fan and Q. Yang, "A Robust Detection Algorithm for Copy-Move Forgery in Digital Images", Forensic Sci. Int., vol. 214, **(2012)**, pp. 33-43.
[22] J. Zhao and J. Guo, "Passive Forensics for Copy-Move Image Forgery Using A Method based on DCT and SVD Forensic" Sci. Int., vol. 233, **(2013)**, pp. 158-66.

[23] 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 IEEE, **(2009)** April, pp. 1053-1056.
[24] G. Lynch, F. Y. Shih and H. Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences, vol. 239, **(2013)**, pp. 253-265.
[25] J. Zhang, Z. Feng and Y. Su, "A new approach for detecting copy-move forgery in digital images", 11th IEEE Singapore International Conference on Communication Systems, ICCS 2008, **(2008)**, pp. 362-366.
[26] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband and K. K. R. Choo, "Copy-move forgery detection: Survey, challenges and future directions", Journal of Network and Computer Applications, vol. 75, **(2016)**, pp. 259-278.
[27] J. Zhao, "Detection of copy-move forgery based on one improved LLE method", 2nd IEEE Int. Conf. Adv. Comput. Control, vol. 4, **(2010)**, pp. 547-550.
[28] J.-C. Lee, "Copy-move image forgery detection based on Gabor magnitude", Journal of Visual Communication and Image Representation, vol. 31, **(2015)**, pp. 320-334.
[29] W. Luo, J. Huang and G. Qiu, "Robust detection of region-duplication forgery in digital image", In 18th international conference on pattern recognition, (ICPR); Hong Kong, **(2006)**, pp. 746-749.
[30] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics", Signal Processing, vol. 91, no. 8, **(2011)**, pp. 1759-1770.
[31] A. Langille and M. Gong, "An efficient match-based duplication detection algorithm", Proc. of the 3rd Canadian conference on computer and robot vision, **(2006)**, pp. 64.
[32] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants", Forensic science international, vol. 171, no. 2, **(2007)**, pp. 180-189.
[33] M. Bashar, K. Noda, N. Ohnishi and K. Mori, "Exploring duplicated regions in natural images", IEEE Trans Image Process, **(2010)**, pp. 1-40.
[34] A. Kashyap and S. D. Joshi, "Detection of Copy-Move Forgery Using Wavelet Decomposition", International Conference on Signal Processing and Communication (ICSC), **(2013)**, pp. 1-3.
[35] Z. Ting and W. Rang-Ding, "Copy-move forgery detection based on SVD in digital image", 2nd International Congress on Image and Signal Processing, CISP'09, **(2009)**, pp. 0-4.
[36] H. Shao, T. Yu, M. Xu and W. Cui, "Image region duplication detection based on circular window expansion and phase correlation", Forensic science international, vol. 222, no. 1, **(2012)**, pp. 71-82.
[37] M. A. Sekeh, M. A., Maarof, M. F. Rohani and B. Mahdian, "Efficient image duplicated region detection model using sequential block clustering", Digital Investigation, vol. 10, no. 1, **(2013)**, pp. 73-84.
[38] H. Huang, W. Guo and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, IEEE, **(2008)**, pp. 272-276.
[39] M. Jaberi, G. Bebis, M. Hussain and G. Muhammad, "Improving The Detection and Localization Of Duplicated Regions In Copy-Move Image Forgery", 18th International Conference on Digital Signal Processing (DSP). IEEE, **(2013)**, pp. 1-6.
[40] X. Bo, W. Junwen, L. Guangjie and D. Yuewei, "Image Copy-Move Forgery Detection Based On SURF", International Conference on Multimedia Information Networking and Security, IEEE, **(2010)**, pp. 889-892.
[41] B. L. Shivakumar and S. Baboo, "Detection of region duplication forgery in digital images using SURF", Int. J. Comput. Sci., vol. 8, **(2011)**, pp. 199-205.
[42] P. Mishra, N. Mishra, S. Sharma and R. Patel, "Region Duplication Forgery Detection Technique Based On SURF and HAC", Sci. World J., **(2013)**.
[43] P. Kakar and N. Sudha, "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", IEEE Trans. Inf. Forensics Secur., vol. 7, **(2012)**, pp. 1018-1028.
[44] L. Chen, W. Lu, J. Ni, W. Sun and J. Huang, "Region Duplication Detection Based On Harris Corner Points and Step Sector Statistics", J. Vis. Commun. Image Represent, vol. 24, **(2013)**, pp. 244-254.
[45] L. Yu, Q. Han and X. Niu, "Feature point-based copy-move forgery detection: covering the non-textured areas. Multimed", Tools Appl., **(2014)**.
[46] 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", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, **(2011)**, pp. 1099-1110.
[47] E. Ardizzone, A. Bruno and G. Mazzola, "Detecting Multiple Copies in Tampered Images", 17th International Conference on Image Processing, **(2010)**, pp. 2117-2120.
[48] T. T. Ng, S. F. Chang and Q. Sun, "A data set of authentic and spliced image blocks", Columbia University, ADVENT Technical Report, **(2004)**, pp. 203-2004.
[49] J. Dong and W. Wang, "CASIA tampered image detection evaluation (TIDE) database, v1. 0 and v2. 0", **(2011)**.
[50] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "CoMoFoD-New database for copy-move forgery detection", In ELMAR, 2013 55th international symposium in IEEE, **(2013)** September, pp. 49-54.

Authors

Saba Mushtaq received her B.E. degree in Electronics and Communications Engineering from Kashmir University, India in 2008. She obtained her M. Tech. degree in Communication and Information Technology from National Institute of Technology, Srinagar, India in 2012. She joined NIT Srinagar in September 2012, as a faculty member. Presently she is a research scholar at NIT Srinagar in Department of Electronics and Communication. Her research interests are Image Processing and Biometrics.

Ajaz Hussain Mir has done his B.E in Electrical Engineering with specialization in Electronics & Communication Engineering (ECE) .He did his M.Tech in Computer Technology and Ph.D both from IIT Delhi in the year 1989 and 1996 respectively. He is Chief Investigator of Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). He has been guiding Ph.D and M.Tech thesis in Security and other related areas and has a number of International publications to his credit Presently he is working as Professor in the Department of Electronics & Communication Engineering at NIT Srinagar, India. His areas of interest are Biometrics; Image processing, Security, Wireless Communication and Networks.