Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Relative Study: Recognition Of Counterfeit Region In An Image

Shashikala S[a] , Dr Ravikumar G K[b]

[a] Department of Computer Science, New Horizon College, Bangalore, Karnataka, 560016, INDIA.

[b] Department of Computer Science and Engineering, BGSIT, Nagamangala 571448, INDIA.

Abstract

This paper reviews significant schemas pertaining to image forensics where the prime emphasize has been laid towards exploring the mechanisms which identify image counterfeit with higher accuracy. The study reviewed the prime contribution published in the last four years and also addressed the unsolved research problems which are needed to be objectified. The extraction of the research gap further extensively elaborated, which identify the gap needed to be filled up. The extensive review of literature also provides better insight into the design aspects associated with the conventional techniques which are defensive against counterfeit image attacks. The future direction of this investigational study aims to come up with a solution model which can address the accuracy and complexity problems which exist in the conventional system.

This paper review significant detection methods, where the prime emphasize has been arranged towards exploring different detection methods and issues with accessibility of advanced picture editing tools today, digital images can be tampered with malicious intention at ease. The image tampering can create various ill effects like false disease diagnosis od medical images, defaming people, hiding evidences, creating false claims etc. It is necessary to ensure the authenticity of the image and detect any counterfeit regions in the image. Nowadays tampering can be done in sophisticated manner without leaving any trace and it becomes difficult to detect with naked eye. In this work, we survey the state of art existing works on

detection of counterfeit or tampered regions in the images. The survey is done to identify the challenges in existing counterfeit detection techniques. The future direction of this comparative study aims to come up with a solution which can address the accuracy.

Introduction

In the digital age, digital images have gained rapid acceptance in various fields like medicine, education, journalism, social media, forensics etc. Images gain visual attention faster than verbal communication and it creates a sense of truthfulness about the event. With rapid availability of image processing technologies, it becomes easy to manipulate digital images with malicious intention. Counterfeiting is the process of manipulating the original image and creating fake image. Image counterfeiting can be done to convey false impression and create disastrous consequences [13]. Image tampering can be done in a sophisticated manner with various photo editing tools and computer programs. The images generated by the faking tools appear natural and authentic. These fake images disrupt the operational and decision-making process. These fake images can assist spreading false propaganda and hide facts. These tools do image tampering without leaving any visual trace to human eyes. Copy-move, splicing etc. are some of the most used digital image forging techniques. Some parts of host image is copied and pasted to different locations in the image in Copy-move forging. Splicing copies some portion from a image and paste it to a different image. Many states of art works have been proposed to detect image tampering. These methods detect tampering by analyzing the structural and statistical changes occurring in the images due to image forgery. The exiting image counterfeit detection methods can be split to three categories

1. Spatial domain-based techniques
2. Frequency domain-based techniques
3. Hybrid techniques

In spatial domain-based techniques, the statistical measures in spatial domain are used to identify the artifacts introduced by counterfeiting. Various features about pixel value and its location are used for counterfeit detection. Frequency domain techniques use wavelet and pixel frequency analysis to identify pixel value and boundary changes introduced by counterfeiting. Hybrid techniques use a mix of spatial, frequency and other image domain techniques to detect counterfeiting regions in the image. Deep learning methods for counterfeit detection are also covered in Hybrid techniques.

The existing methods are analyzed in detail and their pros/cons are identified. The challenges brought by recent image forging methods like deep faking [4] on the counterfeit methods are also discussed in detail. The objective is to identify the challenges in existing counterfeit detection methods and open issues for further research

Related Works

Spatial Domain-based Technique

Li et al (2017) [8] proposed tampering possibility maps for localization of tampered regions. The method is based on improvement of statistical feature-based detector and copy move forgery detector. Possibility map is extracted from each of the detector and a fusion scheme is designed to fuse the individual possibility map to generate a final tampering possibility map. This final tampering possibility map localizes the tampered regions. But the method has higher false positive due to use of statistical features. Y. Li et al (2019) [11] proposed feature point matching algorithm to detect copy move forgery. Key points are extracted from small or smooth regions and matched using novel hierarchical matching strategy to detect the tampered regions. Authors also proposed an iterative localization technique for robustness against orientation, scale and color information for each key point. The approach fails to detect tampered regions even in case of small shape distortion. Mayer et al (2018) [12] proposed an approach to detect copy-paste forgery by observing the inconsistencies in Lateral chromatic aberration (LCA). The approach observers the inconsistency between the global and local estimates of LCA statistically. But the approach fails in case of copy paste forging done with similar images and for smaller regions. Bi et al (2017) [13] proposed a fast offset guided searching method for detection of copy move forgery. Features are extracted from the different regions of image and a initial mapping offset is created. The various combination of reflective offset is created and mapped to initial mapping offset to find copy move forgery. The approach is not transformation variant. Wang et al (2017) [14] proposed a key point-based copy move forgery detection for small smooth regions. Image is segmented to super pixels. Key points are extracted from super pixels and matching key points are detected. The method is able to work in presence of geometric transformations, compression and additive white Gaussian noise. The method is very sensitive to even small distortions in regions. Teerakanok et al (2018) [15] used SURF key points and GLCM feature descriptor to detect copy move forgery. SURF keypoints are extracted from the image. GLCM features are extracted around each SURF area. But the method does not work when the copied region is scaled. Chou et al (2018) [22] proposed a block-based copy move forgery detection strategy. The image is split into regions and local wavelet Gabor wavelet patterns are extracted from the regions. Patterns are matched to detect similar regions. Though the approach is rotation invariant, it does not adapt to scale and has higher false positives.

Frequency domain-based techniques

Guo et al (2018) [7] proposed two methods for detection of fake colorization. Fake colorization is the process of colorizing the gray scale images with realistic color to deceive object recognition applications. This approach is based on the observation that colorized images, compared to natural images possess statistical differences for hue and

saturation channels. Based on this observation histogram-based features are extracted from color channels and thresholding is done to detect fake colorization. But this method is not generic for all fake colorization methods and works only for certain cases. Chen et al (2018) [10] used fractional Zernike moments (Fr ZMs) features for detecting copy-move forging in the images. The image is split to circular overlapping region. For each region, Fr ZMs features are extracted. Features of each patch are matched using a modified Patch Match algorithm to identify similar patches. The similar patches are reported as copy move forging. But this approach cannot detect copy move forgery when copied objects are oriented in different angles. Emam et al (2017) [16] proposed a region duplication forgery detection using difference of Gaussian operator. Covariant key points in the image are extracted using difference of Gaussian operator. Histogram based features are extracted from the key points and matching is done to detect forged regions. But false positives are higher in this method and it cannot detect the case of key point distortion. Zhang et al (2020) [18] proposed a method to detect fake face images generated by Deepfake. The method is based on error analysis of resolution between the face regions and rest of the regions. Most Deepfake methods introduce fake faces with low resolution compared to rest of the resolution in the image. By observing this change, the fake faces in the image are detected. But the method can work only for certain kind of images. If the attacker adds noise to the image, it becomes difficult to detect fake regions. Ghoneim et al (2018) [19] proposed medical image forgery detection using multi resolution regression filtering. Multi resolution regression filtering is applied on the image and features are extracted. The extracted features are classified by support vector machine and extreme learning-based classifier. The work is based on the observation that noise distribution in uniform in the image. In faked region, the distribution of noise is different from rest of the regions. In case of non-uniform noise distribution, the approach fails with higher false positives. Thajeel et al (2019) [20] used quaternion polar complex exponential transform (QPCET) to detect copy move forgery in images. Image is divided into overlapping blocks. QPCET is applied over each block to extract invariant features. The invariant features are then matched with one another using a KD-tree matching algorithm to detect copied regions. Even though the approach is able to work in presence of transformations, noise and blur, it fails for partial occlusions created on the copied regions. Mahmood et al (2018) [23] proposed wavelet features based copy move forgery detection. The image is split to non-overlapping blocks. Stationary wavelet transform features are extracted from each block. The dimension of block is then reduced using DCT. Matching is done feature wise for blocks to detect copied blocks. The method is not scale or rotation invariant. Hosny et al (2017) [24] proposed a copy move forgery of objects in the images. Objects are segmented and smaller objects are removed by applying morphological operators. For the remaining objects, polar complex exponential transform moments are applied to extract features. The features are matched using Euclidean matching. It cannot detect small and smooth region copy.

Hybrid techniques

Islam et al (2020) [5] proposed a hybrid image forgery detection method combining Discrete Cosine Transformation (DCT), Local Binary Pattern (LBP) and a mean operator based feature extraction method. Image is split into non-overlapping blocks. DCT is applied to each block. LBP is applied to magnitude of DCT array to capture changes. Mean value of cell across all LBP block is computed as feature. This feature is classified by Support Vector Machine (SVM) machine learning model to fake or non-fake class. The method was able to achieve 95% fake detection accuracy. But the approach failed for the cases when image was scaled. Also, the approach could work fine only for uncompressed image format. Cristin et al (2018) [6] proposed a hybrid feature extraction method for detecting forgery in face images. Gabor filter, wavelet and texture operator are extracted from the face region of the image. The features are concatenated and classified using SVM classifier. The SVM classifier is optimized using fruit fly optimization algorithm. The method was able to detect fake faces with an accuracy of 95%. This work detects fake based on illumination texture descriptor and it fails when faking is done with uniform illumination texture over the face. Bappy et al (2019) [9] utilized re-sampling features, long short-term memory (LSTM) cells and encoder decoder network to localize the manipulated regions in the image. Spatial maps and frequency domain correlations between manipulated and non-manipulated regions are used by encoder and LSTM network to detect manipulated regions. The method is able to provide pixel wise predictions for image tamper localization. But the method is effective only for splicing tampers. Singh et al (2021) [17] proposed a multi modal framework to detect fake images. Both visual and textual features are used to detect fake images. Intrinsic features learnt from images and latent text feature are matched to verify the authenticity of the image. Textual completeness is needed to detect all fakes in the image. Liu et al (2018) [21] used convolutional kernel network to detect copy move forgeries in the image. The image is segmented into regions and matched using convolution kernel network to detect copied regions. The method performs better than hand crafted features but computation complexity is very high. Also the approach is not scale and transformation variant. Khayeat et al (2020) [20] proposed a deep learning method to detect splicing forgery in the images. Semantic segmentation is done on the image and Haar wavelet level one decomposition is applied onto the segments. Segnet deep learning model is applied on Haar wavelet features to detect splices. The summary of the literature survey is presented in Table 1.

Taxonomy of Research

This work surveys the exiting image forge detection methods in three categories of spatial, frequency and hybrid domain techniques. The taxonomy of the survey is presented in Figure 1.

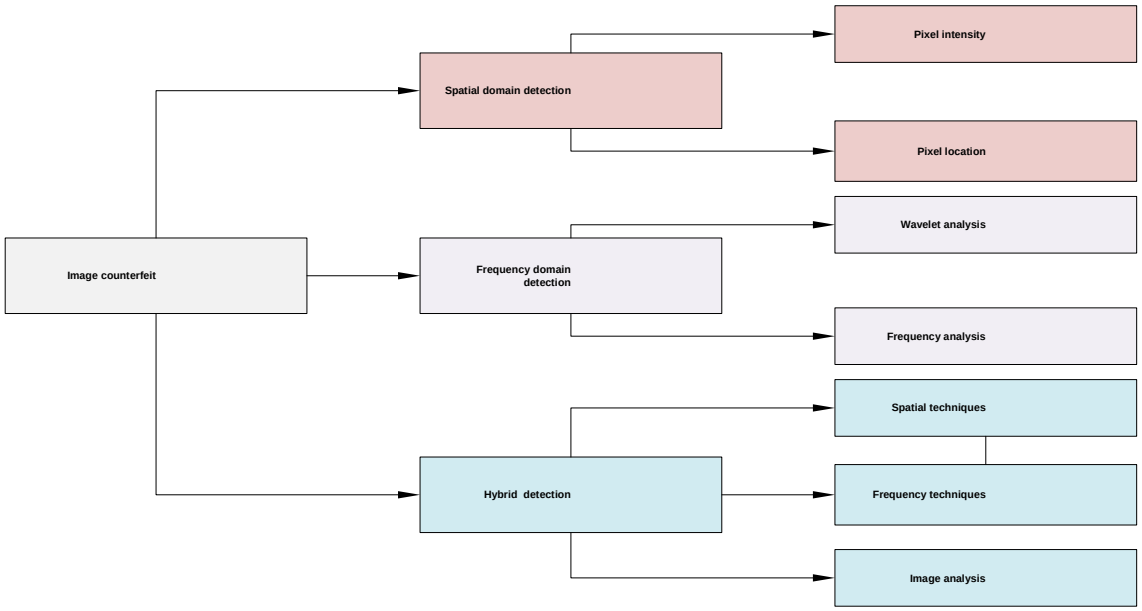

Figure 1 Taxonomy of survey

As seen from Figure 1, image counterfeit techniques are categorized in three categories of spatial domain-based detection, frequency domain-based detection and hybrid techniques. In spatial domain techniques, pixel intensity and pixel location-based techniques were surveyed. In frequency domain techniques, wavelet analysis and frequency analysis techniques were studied. In hybrid techniques combination of spatial, frequency and image analysis in different combinations were studied.

Discussion

The survey of the summary is given below

Table I Summary of survey

Category	Solution	Pros	Cons
Spatial domain techniques	Li et al (2017)	Integrates the advantages of two detector to generate a fused possibility map	Higher false positives due to use of statistical features
	Y. Li et al (2019)	Robust against scale, rotation and color	Fails even for small shape distortion

	Mayer et al (2018)	Color forgery detection using latent chromatic aberration	Approach fails in case of copy paste forging done with similar images and for smaller regions
	Bi et al (2017)	Scale independent forging detection	Fails in case of transformations

	Wang et al (2017)	Key point based detection. Robust for scales, transformations and noises	Very sensitive to even small distortions in regions.
	Teerakanok et al (2018)	SURF based detection with low computational complexity	Fails in case of scaling of copied region.
	Chou et al (2018)	Robust against rotation variants	Higher false positives in case of scaling.
Frequency domain techniques	Guo et al (2018)	Colorization forgery detection	The approach does not work for all kind of images.
	Chen et al (2018)	Circular overlapping regions to reduce computation complexity	Cannot detect when copied objects are oriented in different angles
	Emam et al (2017)	Low computation complexity using difference of Gaussian operator	Higher false positives and fails in case of key point distortion
	Zhang et al (2020)	Can detect Deep fake based on resolution differences in the image	Not generic for all Deep Fakes and fails in case of noises
	Ghoneim et al (2018)	Simple to implement as it is based on observation of noise distribution	In case of non uniform noise distribution the approach fails with higher false positives

	Thajeel et al (2019)	The approach is able to work in presence of transformations, noise and blur	It fails for partial occlusions created on the copied regions.
	Mahmood et al (2018)	Low computational complexity	It cannot detect scale and transformations
	Hosny et al (2017)	Object based detection	Cannot work for small objects or objects with small connective objects
Hybrid techniques	Islam et al (2020)	Higher detection accuracy even for small objects	The approach failed for the cases when image was scaled and it could work well only for uncompressed image format
	Cristin et al (2018)	Can detect fakes based on illumination changes in faces	Fails when contrast operators are applied to the image
	Bappy et al (2019)	Able to provide pixel wise predictions	Works only for splicing forgeries
	Singh et al (2021)	Multi modal for fake detection	Textual completeness is needed to detect all fakes in the image
	Liu et al (2018)	Increased accuracy due to convolutional features	Computation complexity is very high
	Khayeat et al (2020)	Object based forgery detection using Segnet deep learning model	Cannot detect coloration fakes.

From the survey following open issues are identified

1. None of the existing works can detect copy move forgery in case of partial occlusions to the object
2. Very few works on coloration-based forgery
3. Domain specific characteristics are not considered for forgery detection

4. Multi modal approaches lacks semantic correlations to detect forgery 5. Computation complexity is high due to improper region selection strategy.

Each of the issues are discussed in detail below.

Issue 1: Many approaches are proposed to detect forgery in presence of scaling, compression format and transformation. But none of the existing approaches have considered the case of partial occlusion introduced during copy move. The partial occlusion can make the shape of object distorted. This distortion is reflected as big difference in the feature domain. Due to this forgery detection fails.

Issue 2: Coloring based forgeries can be introduced to deceive applications like object recognition, forensics etc. There are very works on coloration forgery detection based on chromatic analysis. But they can be deceived easily by introducing noises.

Issue 3: Most of the approaches are generic and don't consider domain specific characteristics in forgery detection. Say artificial tumor is introduced in the medical image, domain knowledge can be applied to detect if the location of tumor is valid for this specific body part. This kind of domain specific characteristics can help to detect sophisticated copy move forgeries. Domain specific characteristics can help to identify Deepfakes.
Issue 4: Multi modal approaches use information from meta-data in addition to image characteristics to detect forgery. The advantages of the multi modal approaches can be leveraged to the maximum, only if semantic context is established for correlating the metadata and the image semantics. Currently there are no works addressing the problem of semantic correlation in multi modal based forgery detection.

Issue 5: Most of the approaches split the images to non-overlapping blocks or overlapping regions. With the increase in the number of regions, the time for feature extraction and matching also increases. Considering the requirement of detection in presence of scale, transformations etc the detection time shoot up. This can be optimized by a region selection strategy. This region selection strategy can be based on domain specific characteristics and metadata information. Currently there are no works addressing this problem of region selection for forgery detection.
Recently deep learning is used for detecting image counterfeits. A comprehensive summary of deep learning methods for copy move forgery detection are proposed in [27]. A recent deep learning method for copy move detection is presented in [26]. But the most recent deep learning approach too did not address the issues considered in this work. The recent approach too did not consider the copy move forgery in case of partial occlusions.
Conclusion

The current works on image counterfeit detection are explored in this work. The survey is conducted in three categories of spatial domain, frequency domain and hybrid techniques. The pros and cons in each of the solution are identified. The open issues in exiting works on forgery detection are identified and detailed. Further work will be on designing efficient solutions to address the identified open issues.

References

1. Mallonee L, Infamously, Altered Photos, Before and After Their Edits. Wired. Available online: https://bit.ly/2Ia8zqf., (2015).
2. Wikipedia contributors List of Photo Manipulation Controversies. Wikipedia, Available online: https://bit.ly/2wcweBB(2019).
3. Allbeson, T, Allan, S, Springer International Publishing: Berlin/Heidelberg, Germany. pp. 69–84, (2019).
4. Westerlund, Mika, Technology Innovation Management Review. 9. 39-52, 10.22215/timreview/1282., (2019).
5. Islam, M.M,Karmakar, G,Kamruzzaman, and JMurshed, M, Electronics. 9, 1500,(2020).
6. R. Cristin, J. P. Ananth and V. Cyril Raj, in IET Image Processing, vol. 12, no. 8, pp. 1439-1449, (2018).
7. Y. Guo, X. Cao, W. Zhang and R. Wang, in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 1932-1944, (2018).
8. H. Li, W. Luo, X. Qiu and J. Huang, in IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1240-1252, (May 2017).
9. J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath and A. K. Roy-Chowdhury, in IEEE Transactions on Image Processing, vol. 28, no. 7, pp. 3286-3300, (2019).
10. B. Chen, M. Yu, Q. Su, H. J. Shim and Y. Shi, in IEEE Access, vol. 6, pp. 56637-56646, (2018).
11. Y. Li., & J. Zhou,in IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1307-1322, (2019).
12. O. Mayer, & M. C. Stamm, in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1762-1777, (2018).
13. X. Bi, & C.-M. Pun, in Inf. Sci, vols. 418–419, pp. 531–545, (2017)
14. X.Y. Wang, S. Li, Y.-N. Liu, Y. Niu, H.-Y. Yang, and Z.L Zhou, in Multimedia. Tools Appl, vol. 76, no. 22, pp. 23353–23382, (2017).
15. S. Teerakanoko, T. Uehara, in Proc. COMPSAC, pp. 365–369, (2018).
16. M. Emam, Q. Han, Q. Li, and H. Zhang, in Proc. ICCSS, London, U.K, pp. 119–123, (2017)
17. Singh, B and Sharma, D.K, in Neural Computer &Application, (2021).
18. Weiguo Zhang,Chenggang Zhao and Yuxing Li, Entropy (Basel, Switzerland) vol. 22,2 249,(2020).

19. Ghoneim A Muhammad G,Amin S U and Gupta B, in IEEE Communication Magazine,56(4),33-37,(2018).
20. Thajeel, Salam Shakir, Ali , Rasheed, Waleed, Sulong and Fhazali, in KSII Transactions on Internet and Information Systems.13.4005-4025. 10.3837/tiis.2019.08.010, (2019).
21. Liu Y., Q. Guan, and X. Zhao, in Multimedia Tools and Applications, vol. 77, no. 14, pp. 18269-18293., (2018).
22. Chou, C.L. and J.C. Lee, in Proc. of Springer on International Conference on Security with Intelligent Computing and Big-data Services, vol. 733, pp 47-56, (2018).
23. Toqeer Mehamood, Zahid mehmood, Tanzilla Saba and Mohsin Shah, in Journal of Visual Communication and Image. Representation, vol. 53, pp. 202-214, (2018).
24. Hosny, K.M., H.M. Hamza and N.A. Lashin, in The Imaging Science Journal, vol. 66, no. 6, pp. 330-345, (2017).
25. Ahmed Abdullahadi Ahmed Al-Moadhen, Ridha, Mustafa, and Khayeat Ali, in AIP Conference Proceedings. 2290. 10.1063/5.0027442., (2020).
26. Rodriguez-Ortega., Yohanna, and Ballesteros, Dora and Renza, Diego, in Journal of Imaging.7.59. 0.3390/jimaging7030059, (2021).
27. B. Z. Abidin, H. B. A. Majid, A. B. A. Samah and H. B. Hashim, 6th International Conference on Research and Innovation in Information Systems (ICRIIS), pp. 1-6, doi:10.1109/ICRIIS48246.2019.9073569, (2019).