Survey of Image Tampering Detection

Vivek Kumar Nema[1], Prachi Parwar [2]
Department of CSE
[1,2] Takshshila Institute of Engineering and Technology, Jabalpur

Abstract- *In multimedia forensics, many efforts have been made to detect whether an image is pristine or manipulated with high enough accuracies based on specially designed features and classifiers in the past decade. Editing a real-world photo through computer software or mobile applications is one of the easiest things one can do today before sharing the doctored image on one's social networking sites. Although most people do it for fun, it is suspectable if one concealed an object or changed someone's face within the image. Before questioning the intention behind the editing operations, we need to first identify how and which part of the image has been manipulated. It therefore demands automatic tools for identifying the intrinsic difference between authentic images and tampered images. However, the important task for localizing the tampering regions in a fake image still faces more challenges compared with the manipulation detection and relatively a few algorithms attempt to tackle it.*

Keywords- Image tampering detection; image forgery detection; image forensics; image copy-move detection; image splicing detection, CNN.

I. INTRODUCTION

With the rapid technological advancement has strengthened the growth of every field imaginable, security being one of them, it has also become easy to breach it. Not only can legal documents be stolen and forged, criminal evidence- such as photographs and security footage can be easily tampered with. One may feel it is enough for an institution to check ID's at the front gate but they do not realize how menial of a task it is for a criminal to get their hands on fake ID's. Posing as someone else in a public setting is a trouble free task even for amateur criminals. As mentioned before, photo editing tools which on top being easily accessible are also extremely friendly. One can learn basic photo editing tips in a few hours, even if they have never seen an image editing software before. There is nothing too advanced about photo editing anymore, whereas forgery has become even more difficult to detect.

Image forgeries may be classified into many types such as copy-move forgery, splicing and many more. Research has been going on in this field for years now and many effective methods have been proposed to detect such forgeries. Xuedong Zhao et al. proposed a method for colour channel design to find the most inequitable channel, which they called the optimal chroma-like channel, for feature extraction [1]. Another process to detect counterfeited documents, mainly tampered with using a photocopier, is through superimposition [2]. However, such techniques have now become obsolete since forgery these days is digital, clean and indistinguishable to the human eye. Therefore, machines are a more viable option now. Most of the techniques used to detect those manipulations employ machine learning and pattern recognition [3]. Region duplication can be detected by calculating the scale invariant feature transform (SIFT) key-points and then finding all the pixels within the duplicated region [4]. Digital documents that have been rotated, scaled or resized can also be detected easily using image processing tools [5].

Research has been done so far to detect duplicated regions in a document tampered using copy-move forgery with the help of block-based and traditional key-point based methods [6]. Since all the databases in a security system are digital, people mostly rely on the image features that can be extracted easily. For instance, gradient based texture features, with the help of a machine, can easily be calculated and compared [7]. Another devised scheme is to divide the image into overlapping blocks, thinking of them as vectors and find the manipulated region through radix sorting [8]. Image forgery detection can also be done using only image processing and without any embedded security information. This method makes use of Fuzzy Transform (F-Transform) and Ring Projection Transform (RPT) to detect forgeries. These transforms convert the data to a single dimension significantly reducing the computational capacity [9]. Various studies have also been done weighing down the pros and cons of the prevalent copy-move forgery detection (CMFD) techniques [10]. Image processing algorithms such as DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) are one of the many feature extraction methods that are used today to detect forged images [11]. Another approach to detected tampered images is to make use block based methods, but by using the non-overlapping texture blocks as a base for the smooth blocks, thus reducing the computational capacity [12]. Copy-move forgery (CMF) can also be detected using algorithm based on Stationary Wavelet Transform (SWT), which is able to accurately detect the duplicated blocks [13]. CMF can also be detected easily if the feature vector generated is based on colour perception and object representation [14]. Reflective SIFT based algorithms are also proficient in detecting duplicated blocks in copy-move forgeries [15].

II. CLASSIFICATION OF IMAGE FORGERY

With creativity and understanding of the properties of image only, tampering of images becomes successful. Tampered images are used not only to create incredible photos for fun, but also in various other walks of life like providing security to valid documents with watermarks or digital signatures. No matter whatever the cause of act might be, the forger should use a single or a combination of series of image processing operations. To detect image tampering, the knowledge of tampering operations is essential. Image forgery techniques are classified in to two: Active and passive approaches [16]. Figure2.1 shows the major classification of image forgery.

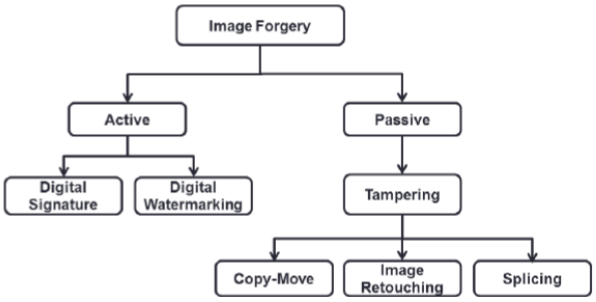

Figure 2.1: Classification of image forgery

III. IMAGE FORGERY DETECTION METHODS

The invisible forged image detection is highly sophisticated. Any forgery introduces a correlation among the forged image segments and the original segment which can be used for successful forgery detection. Several efficient forgery detection methods are introduced for passive image forgery detection. It is mainly classified into three.

1) Image retouching: it is considered as a less harmful type of image forgery. In this method instead of completely changing the image, it enhances or reduces certain feature of the image. This method is popular among magazine photo editors.
2) Copy move forgery: in this method a part of the image is copied and pasted into another part of the same image. A copy-move forgery is the process, where one copies a particular region of a digital image and pastes the region on top of another region within the same image. It is usually used for duplicating an object within an image, after proper post-processing. Such tampering images where a region of an image is copied from one part and is moved to another part in the same image [17] give rise to copy-move forgery. The copied region can be processed with techniques like rotation, scaling, etc. Such techniques are used to make it hard for the human eyes to discover the forgery. In image forensics, the detection of copy-move forgeries has become a highly researched topic.
3) Image splicing: it is the most common image tampering operation. In this part two or more different images are combined together to form a new image and it is very difficult to identify. Most important type of splicing consist of images of people, that is images of two people in two different images are combined to form a new image. Image splicing is fundamentally different from copy-move in the sense that the pasted region cannot be found elsewhere within the same image. Such a fundamental difference also makes it harder to detect image splicing forgeries than to detect copy-move forgeries. Because it is easier to detect similar contours of an object within the same image due to image properties such as texture, color, size, shape etc will have a resemblance, whereas, in case of image splicing, the newly pasted object contour will have different image properties. If an image is authentic that means it should be captured by a single camera. There are different methods to identify whether an image is authentic or not. If the image is authentic there is a consistent relation between every pixel in that photo, if it is tampered there is an inconsistent relation between every pixel in an image. By identifying this inconsistency, tampered image can be detected.

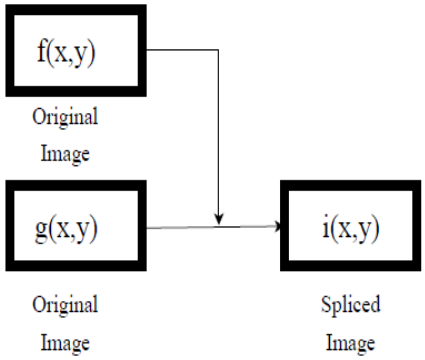

Figure 3.1: Image Splicing

A digital image is a representation of a two-dimensional image as a finite set of digital values. The units for such digital representation are called picture elements or pixels. Resolution of an image is an important property for describing a digital image. It is related to the number of unit pixels in a spatial measurement. The resolution of a digital camera is simply the multiplication of the width and height of the pixel dimensions (or, the number of columns and the number of rows respectively). There are many common digital image tampering techniques.

Transformations Applied for Pre-processing of Digital Image:

The following transformations were applied on the CASIA v2.0 dataset for different experiments:

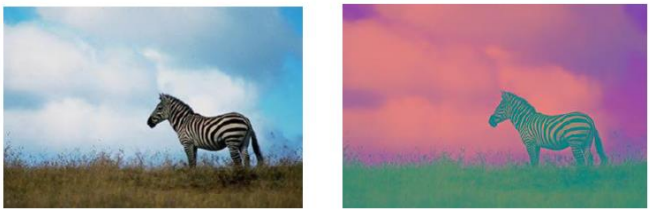

Figure 3.2: Image Transformation Mechanism

Machine learning, a convolutional neural network (CNN or ConvNet) is a class of deep feed-forward artificial neural networks utilizing convolutional layers. Nonlinear, pooling/down sampling, fully-connected layers are also usually integrated among the convolutional layers. CNNs maintain the property of being shift variant and partial transformation variant (dependent on the training data). This way CNNs allow lower layers to learn local features and with the help of local connectivity higher layers learn high level features. CNNs are widely used in many applications in computer vision.

1) Maxpooling: Max pooling is a sample-based discretization process. It is used for reducing dimensions of the input features. However, to prevent the loss of relevant features, the features are down-sampled in a way so that most dominant image features are retained. Such reduction in dimensionality helps to reduce the number of parameters.
2) Filters: A filter is a vector of weights with which we convolve the input image.

IV. RELATED WORK

With the development of imaging and computer graphics technologies, transmission of the massive video data volume [18], [19] and video data security have both become challenges. Editing or tampering with digital videos (images) has become easier, even for an inexperienced forger, with the aid of multimedia editing software. A potential rise in multimedia tampering can seriously affect the security of our society. Therefore, multimedia information security [20]–[23] and multimedia forensics [24]–[27] have become important topics.
In contrast to the active multimedia forensic approaches, e.g., digital watermarking [28] and signatures [29], passive techniques for video (image) forensics are more challenging. As no additional information is embedded into the original video (image) in advance. Although digital forges may leave no visual clues regarding what might have been tampered with, they may alter the underlying statistics. In recognition of this fact, a variety of tampering detection techniques have been proposed in recent years, such as recompression detection [30], copy move detection, and splicing detection. Because JPEG is the most popular image format, passive JPEG image tampering detection has attracted much research interest. Since the blocking artifacts introduced by JPEG compression will change considerably if tampering operations exist, Ye et al. [31] measured the symmetrical property of the blocking artifacts by computing a blocking artifact characteristics matrix (BACM) in a suspicious JPEG image as evidence of tampering.

Farid [32] proposed to detect tampered regions for a double compressed JPEG image by recompressing the image at different quality levels and looking for the presence of so-called ghosts. Wang et al. [33] observed that the quantization noise of high frequency DCT coefficients in a tampered region is stronger than an unchanged region, and they subsequently utilized this feature to locate tampered regions.

In recent years, deep neural networks, such as the deep belief network, deep auto encoder and convolutional neural network (CNN), have shown to be capable of extracting complex statistical dependencies from high dimensional sensory inputs and efficiently learning their hierarchical representations; this capability allows these methods to generalize well across a wide variety of computer vision (CV) tasks, including image classification, speech recognition, and image restoration [34]. However, with the development of graphics processing units (GPUs) and the availability of large-scale training datasets, it is reasonable that the forgery might take these powerful manipulation methods based on deep learning to cover the JPEG artifacts, which might cause the fail of traditional forensics methods. Hence, it is necessary to study the forensics of deblocking. Motion JPEG (MJPEG) is one of the most popular video formats, in which each video frame or interlaced field of a digital video sequence is compressed separately as a JPEG image. In this paper, we propose a novel image deblocking detection approach that can detect deblocking and automatically learn feature representations based on a deep learning framework. We train a supervised CNN to learn the hierarchical features of deblocking operations with labeled patches from the training dataset. The first convolutional layer of the CNN serves as the preprocessing module to efficiently obtain the tampering artifacts. Instead of a random strategy, the kernel weights of the first layer are initialized with 23 high-pass filters used in the calculation of residual maps, which helps to obtain the tampering artifacts. We then extract the features on the basis of a patch by applying a patch-sized sliding window to scan the whole image. The generated image representation is then condensed by regional pooling to obtain the discriminative feature.

Image forgery detection is a massive field in forensic and signal processing. Basic classification and localization solutions for image forgery have produced a huge number of

papers since 2010. Most work in literature revolves around patch classification and using the classifiers to localize where image forgery took place. Recent works are focused on localization using different datasets.

A. Signal processing based methods

Earlier image forgery detection research is focused on signal processing. Therefore, many methods are proposed using interpolation marker [35]–[37]. In [38], Gallagher et al. exploit the second order derivative of image to expose the periodicity in the variance function generated by interpolation. A major downside of this method is that it cannot be applied to rotated or skewed images. Based on this, an improved approach is developed by Mahdian et al. [38]. They introduce the Radon transform and auto-covariance to make the algorithm suitable for rotated or skewed images. Although the method is more generalized, it still focuses on uncompressed images. Luo et al. [39] propose a framework for detecting the tampered region in compressed images. Their method first decompresses images and then evaluates the interpolation marker. Wu et al. [40] use a metrology method to infer the forged regions. Although it can be applied to different image formats, one major limitation is that the method is somewhat limited in recovering of camera calibration. A specific geometric interpretation is required to be evaluated first in order to recover the said calibration. A pyramid transforms (SPT) and local binary pattern (LBP) based method was proposed in [41]. SPT is used for discovering sub bands that make up the whole image. These sub bands usually have different intensity and angle. These sub bands are then exploited to extract LBP histograms. The intention is to use these histograms as features. An SVM classifier with linear kernel is used with these extracted features to train a binary classifier. Curvelet transform by replacing the SPT was found to be a better solution while keeping the LBP histogram phase intact. Their methods were evaluated in CASIA databases which is also the target of our project. The authors in [42] also train an SVM classifier using features extracted maximum between-class separation of pixel pair histograms and Fourier Transform to achieve high classification rate. Gabor wavelets were the focus of the study by the authors in [43]. Only the magnitudes of these wavelets were considered. Extracted histogram Gabor magnitude after principal component analysis was fed into a statistical model. Fourier Mellin transforms results especially in copy-move image forgery detection. Compound statistical features were utilized by the authors in [44]. A wavelet-based de-noising filer was applied to extract sensor pattern noise image, which formed the basis of the compound features. The authors in [45] targeted to reduce false positives by exploiting multi-resolution LBP. An agreement protocol among random samples was maintained too for the said purpose.

B. Deep Learning based methods

In recent years, researchers begin to exploit deep learning based models, e.g. [46]–[48]. Deep learning based models are highly utilized for forged image segmentation and localization problems. Many of these models utilize the re-sampling features in image forgery detection. Therefore, the major weaknesses of these methods are similar to signal processing based methods. In an effort to be independent from re-sampling features, methods in, directly apply the neural network on the original images. Attempt to use a 10-layer CNN and use an auto encoder to perform forged image patch localization. However, their methods are prone to Overfitting on patch datasets. Employ a hybrid CNNLSTM-CNN model to capture discriminative features between the tampered and original regions. Their method focuses on the difference between edges, especially the difference of sharpness. While the sharpness of edges is a good indicator to classify tampered regions in high resolution images, it is not effective in low resolution images that are rather smooth. Gholap and Bora described dichromatic deflection method for forgery detection. It is obtained by reflection from the image. There are mainly two types of reflection from an image they are surface reflection and interface reflection. It estimates the intersection points in dichromatic deflection model. If it is greater than threshold it is identified as spliced image. Francis, Gholap and Bora identified splicing by detecting inconsistency in nose regions of the human present in the image, which is also based on dichromatic deflection model.

Fang and Xuemin uses illuminant color to identify splicing. In this method GGE is used for illuminant color estimation. Here entire images divided into different blocks, and then the inconsistent region is identified by measuring an error angle. If this error angle is greater than threshold, it is identified as spliced. Tan et al.proposed that illuminate map can be estimated by Inverse intensity chromaticity (IIC). Faridet al detected real image by identifying inconsistency in shadow. It is based on the assumption that most forms of tampering will change statistical property of the image. Most of these images are in JPEG format. JPEG compression introduces blocking artifacts in the image. Authenticity of animate was detected by identifying the inconsistency in blocking artifacts.

REFERENCES

[1] Zhao, X., Li, S., Wang, S., Li, J., & Yang, K. (2012) , Optimal chroma-like channel design for passive colour image splicing detection, EURASIP Journal on Advances in Signal Processing, 2012(1), 240.

[2] Joshi MC, Kumar A, Thakur S. Examination of digitally manipulated-machine generated document, a case study

elucidating the issue of such unwanted progenies of modern technology. Prob Forensic Science 2011; 56:162–73.

[3] Qureshi, Muhammad Ali, and Mohamed Deriche, A bibliography of pixel-based blind image forgery detection techniques, Signal Processing: Image Communication 39 (2015): 46-74.

[4] Xunyu Pan, SiweiLyu, "Region Duplication Detection Using Image Feature Matching", Information Forensics and Security IEEE Transactions on, vol. 5, pp. 857-867, 2010, ISSN 1556-6013.

[5] Anil Dada Warbhe, Rajiv V. Dharaskar, Vilas M. Thakare, "Digital image forensics: An affine transform robust copy-paste tampering detection", Intelligent Systems and Control (ISCO) 2016 10th International Conference on, pp. 1-5, 2016.

[6] Mohsen Zandi, Ahmad Mahmoudi- Aznaveh, AlirezaTalebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector", Information Forensics and Security IEEE Transactions on, vol. 11, pp. 2499-2512, 2016, ISSN 1556-6013.

[7] Xia, Z., Lv, R., Zhu, Y., Ji, P., Sun, H., & Shi, Y. Q. (2017), Fingerprint liveness detection using gradient-based texture features. Signal, Image and Video Processing, 11(2), 381-388.

[8] Lin, Hwei-Jen & Wang, Chun-Wei & Kao, Yang-Ta. (2009) Fast copy-move forgery detection WSEAS Transactions on Signal Processing. 5. 188-197.

[9] Ansari, MohdDilshad&PrakashGhrera, Satya. (2018). Copymove image forgery detection using direct fuzzy transform and ring projection.International Journal of Signal and Imaging Systems Engineering. 11. 44. 10.1504/IJSISE.2018.10011742.

[10] BadalSoni, Pradip K. Das, Dalton Meitei Thounaojam. (2018) CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. IET Image Processing 12:2, pages 167-178.

[11] Jawadul H. Bappy, Amit K. Roy-Chowdhury, Jason Bunk, LakshmananNataraj, B.S. Manjunath. Exploiting Spatial Structure for Localizing Manipulated Image Regions. (2017) IEEE International Conference on Computer Vision (ICCV), pages 4980- 4989.

[12] Hajihashemi, Vahid&Gharabagh, Abdorreza. (2018). A Fast, Block Based, Copy-Move Forgery Detection Approach Using Image Gradient and Modified K-Means. 298-307. 10.1007/978-3-319-68385-0_25.

[13] Mahmood, Toqeer& Nawaz Tabassam&Mehmood, Zahid&Khan, Zakir& Shah, Mohsin& Ashraf, Rehan. (2016). Forensic analysis of copy-move forgery in digital images using the stationary wavelets.578-58310.1109/INTECH.2016.7845040.

[14] Kushol, Rafsanjany&Salekin, MdSirajus&HasanulKabir, Md&Alam Khan, Ashraful. (2016). Copy-Move Forgery Detection Using Colour Space and Moment Invariants-Based Features.1-6.10.1109/DICTA.2016.7797027.

[15] Agarwal, Vanita& Mane, Vanita. (2016). Reflective SIFT for improving the detection of copy-move image forgery.84-88.10.1109/ICRCICN.2016.7813636.

[16] NishthaParashar and NirupamaTiwari, A Survey of Digital Image Tampering Techniques, International Journal of Signal Processing, 2015, Vol.8, No.10, Pp.91-96.

[17] R. Wadhwa and M. T. Scholar, "Image Quality Assessment for Fake Biometric Detection," IJSRD - International J. Sci. Res. Dev., vol. 2, no. 03online, pp. 2321–613, 2014.

[18] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, ''Adaptive fractional-pixel motion estimation skipped algorithm for efficient HEVC motion estimation,'' ACM Trans. Multimedia Comput. Commun.Appl., vol. 14, no. 1, pp. 1–19, 2018.

[19] Z. Pan, X. Yi, and L. Chen, ''Motion and disparity vectors early determination for texture video in 3D-HEVC,'' Multimedia Tools Appl., pp. 1–18, Nov. 2018. doi: 10.1007/s11042-018-6830-7.

[20] Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, ''On the fault-tolerant performance for a class of robust image steganography,'' Signal Process., vol. 146, pp. 99–111, May 2018.

[21] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, ''Selection of rich model steganalysis features based on decision rough set α-positive region reduction,'' IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 336–350, Feb. 2019.

[22] J. Chen, W. Lu, Y. Fang, X. Liu, Y. Yeung, and Y. Xue, ''Binary image steganalysis based on local texture pattern,'' J. Vis. Commun. Image Represent, vol. 55, pp. 149–156, Aug. 2018.

[23] F. Zhang, W. Lu, H. Liu, and F. Xue, ''Natural image deblurring based on L0-regularization and kernel shape optimization,'' Multimedia Tools Appl., vol. 77, no. 20, pp. 26239–26257, 2018.

[24] X. Liu, W. Lu, Q. Zhang, J. Huang, and Y.-Q. Shi, ''Downscaling factor estimation on pre-jpeg compressed images,'' IEEE Trans. Circuits Syst. Video Technol., to be published. doi: 10.1109/TCSVT.2019.2893353.

[25] X. Liu, W. Lu, T. Huang, H. Liu, Y. Xue, and Y. Yeung, ''Scaling factor estimation on jpeg compressed images by cyclostationarity analysis,'' Multimedia Tools Appl., pp. 1–18, Jul. 2018. doi: 10.1007/s11042-018- 6411-9.

[26] J. Li, W. Lu, J. Weng, Y. Mao, and G. Li, ''Double JPEG compression detection based on block statistics,'' Multimedia Tools Appl., vol. 77, no. 24, pp. 31895–31910, 2018.

[27] C. Lin, W. Lu, W. Sun, J. Zeng, T. Xu, and J. H. Lai, ‘‘Region duplication detection based on image segmentation and keypoint contexts,’’ Multimedia Tools Appl., vol. 77, no. 11, pp. 14241–14258, 2018.

[28] C. Vyas and M. Lunagaria, ‘‘A review on methods for image authentication and visual cryptography in digital image watermarking,’’ in Proc. IEEE Int. Conf. Comput.Intell.Comput. Res., Coimbatore, India, Dec. 2014, pp. 1–6.

[29] F. Xue, Z. Ye, W. Lu, H. Liu, and B. Li, ‘‘MSE period based estimation of first quantization step in double compressed JPEG images,’’ Signal Process. Image Commun., vol. 57, pp. 76–83, Sep. 2017.

[30] S. Ye, Q. Sun, and E.-C. Chang, ‘‘Detecting digital image forgeries by measuring inconsistencies of blocking artifact,’’ in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 12–15.

[31] H. Farid, ‘‘Exposing digital forgeries from JPEG ghosts,’’ IEEE Trans. Inf.Forensics Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[32] W. Wang, J. Dong, and T. Tan, ‘‘Tampered region localization of digital color images based on JPEG compression noise,’’ in Proc. Int. Conf. Digit.Watermarking. Berlin, Germany: Springer, 2011, pp. 120–133.

[33] Y. Tai, J. Yang, X. Liu, and C. Xu, ‘‘MemNet: A persistent memory network for image restoration,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Oct. 2017, pp. 4549–4557.

[34] Alin C Popescu and HanyFarid, Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on signal processing, 53(2):758–767, 2005

[35] Alin C Popescu and HanyFarid. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10):3948–3959, 2005.

[36] S Prasad and KR Ramakrishna. On resampling detection and its application to detect image tampering. In Multimedia and Expo, 2006 IEEE International Conference on, 2006.

[37] Andrew C Gallagher. Detection of linear and cubic interpolation in jpeg compressed images. In Computer and Robot Vision, Proceedings.The 2nd Canadian Conference on, 2005.

[38] BabakMahdian and StanislavSaic, Blind authentication using periodic properties of interpolation. IEEE Transactions on Information Forensics and Security, 3(3):529–538, 2008.

[39] JieboLuo and Andrew C Gallagher, Detecting compositing in a previously compressed image, May 18 2010. US Patent 7,720,288.

[40] Lin Wu, Xiaochun Cao, Wei Zhang, and Yang Wang, Detecting image forgeries using metrology. Machine Vision and Applications,23(2):363– 373, 2012.

[41] Pan, SinnoJialin, and Qiang Yang. ”A survey on transfer learning”, IEEE Transactions on knowledge and data engineering 22.10 (2010): 1345-1359.

[42] Shabanifard, Mahmood, Mahrokh G. Shayesteh, and Mohammad Ali Akhaee. ”Forensic detection of image manipulation using the Zernike moments and pixel-pair histogram.” IET Image Processing 7.9 (2013): 817-828.

[43] Isaac, Meera Mary, and M. Wilscy. ”Image forgery detection based on Gabor Wavelets and Local Phase Quantization”, Procedia Computer Science 58 (2015): 76-83.

[44] Li, Chang-Tsun. ”Source camera identification using enhanced sensor pattern noise.” IEEE Transactions on Information Forensics and Security 5.2 (2010): 280-287.

[45] Jawadul H Bappy, Amit K Roy-Chowdhury, Jason Bunk, LakshmananNataraj, and BS Manjunath. Exploiting spatial structure for localizing manipulated image regions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017.

[46] Belhassen Bayar and Matthew C Stamm.A deep learning approach to universal image manipulation detection using a new convolutional layer.In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016.

[47] Belhassen Bayar and Matthew C Stamm.On the robustness of constrained convolutional neural networks to jpeg post compression for image resampling detection. In Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on, 2017.

[48] Yuan Rao and Jiangqun Ni, A deep learning approach to detection of splicing and copy-move forgeries in images. In Information Forensics and Security (WIFS), IEEE International Workshop on, 2016.