International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 3, March-April 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Review on Various Forgery Detection Techniques

Aarushi Thusu[1], Mr. B. Indra Thannaya[2]

[1]M.Tech Scholar, [2]Assistant Professor,
[1,2]Department of Computer Science Engineering,
Indira Gandhi Delhi Technical University for Women, New Delhi, Delhi, India

ABSTRACT

Nowadays, there barely exists any platform where digital images are not used. They are used in almost every field, namely digital media, electronic media, military, law, industry, forensics, and so on, and all over the internet. With such vast numbers of images, the importance of their authenticity has increased enormously .We give much importance to what we see on daily basis in newspapers, on the covers of magazines, social media such as Facebook, Instagram, Twitter and many more. Digital image manipulation is the act of distorting the contents of an image in order to fulfil some fraudulent purposes, such manipulations are known as forgeries. There exist various cases of image forgeries in history which caused clutter and affected people/ organizations. Earlier photographers were habituated with using the process of photomontage, in which composites of images were created by pasting, gluing to get the final print. However, due to evolution of technology, various tools have been developed by researchers and made available over the internet.

How to cite this paper: Aarushi Thusu | Mr. B. Indra Thannaya "A Review on Various Forgery Detection Techniques" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-3, April 2022, pp.2119-2129, URL: www.ijtsrd.com/papers/ijtsrd49915.pdf

IJTSRD49915

I. INTRODUCTION

Nowadays, there barely exists any platform where digital images are not used. They are used in almost every field, namely digital media, electronic media, military, law, industry, forensics, science and technology, medical sciences, glamour, social media, and so on, and all over the internet. With such vast numbers of images, the importance of their authenticity has increased enormously. There is a belief that the image speaks more truth about the incident or the situation captured than the words. An image can more strongly influence viewers than millions of words; images are used as evidence in courts, scientific research, political campaigns and celebrity magazines. The rapid availability, ease of use and wealth of inexpensive devices to capture, store and send images (mobile devices, digital cameras and scanners) have helped to spread them.

II. THE NEED FOR THE DETECTION OF DIGITAL FORGERIES

Digital image manipulation [1,2] is the act of distorting the contents of an image in order to fulfil some malevolent/fraudulent purposes. The problem of image forgeries is not new, but is as old as images themselves. There exist various cases of image forgeries in history [3] which caused clutter and affected people/organizations. Earlier photographers were habituated with using the process of photomontage, in which composites of images were created by pasting, gluing, overlapping and reordering two or more photographs to get the final print that looks like just a single photograph (Figure1). Due to the evolution of technology, various photo manipulation tools have been developed by researchers and programmers and made available over the internet. Various professional/amateur digital image editing tools are available, such as Affinity Photo, Paint shop, Adobe Photoshop, GIMP, Photoshop Elements, and many more. Some of them are available for free and a few are paid for but easily accessible and affordable. Further, images edited using the software tools are subjected to several processing stages and are so photorealistic that, it is almost impossible for human vision system to recognize shows grave susceptibility as well as decreases the trustworthiness of the digital images.

Devising effective and real-time detection and localization methods is currently important as these forgery attacks are increasing with time [4].

Figure 1: Photomontage of kiwi fruit and lemons digitally manipulated using GIMP

III. IMAGE FORGERY AND TYPES OF DIGITAL IMAGE FORGERY

Image forgery refers to the deliberate manipulation of a digital image, for the only purpose of amending the semantic of the visual message comprised in that image. There have been different techniques utilized for forging an image. Digital image forgery can be classified into three primary methods: Copy-Move forgery, Image splicing, and Image resampling.

IV. COPY-MOVE (CLONING) FORGERY

Copy-move is the popular and most common kind of image tampering technique [5]. Copying from one part and pasting the same in some other part in the same image with an intention to hide certain content in the original image.

An example of copy-move attack is shown in figure 2 where left side shows original image which contains three rockets and right side shows forged imaged with four rockets.

Figure 2: Copy-move Image Forgery

V. IMAGE SPLICING

Image splicing is a commonly used forgery technique in image tampering [6]. Splicing is a form of photographic manipulation in which the fragments of same or different images are combined to produce a single composite image (forged image) without further post processing such as smoothening of boundaries among different fragments.

VI. IMAGE RETOUCHING

Retouching involves a lot of treatments like basic colour correction, glamour retouching, skin retouching, photo restoration, photo cartooning etc. Example is shown below in figure 3, where real face is on the left and right shows the retouched version of it.

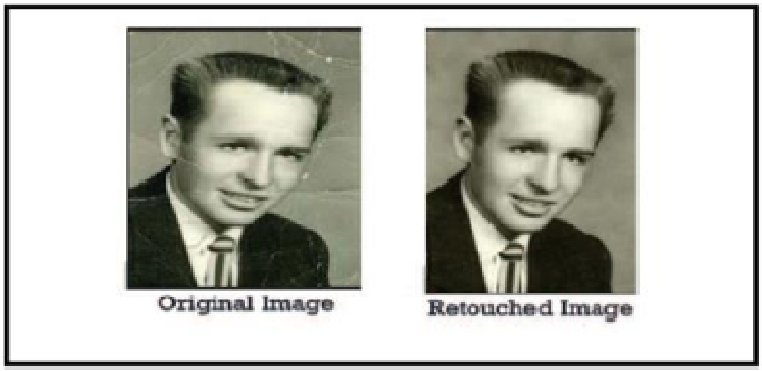


Figure 3: Image Retouching

VII. CLASSIFICATION OF DETECTION TECHNIQUES

Researchers have proposed various techniques to detect the forgery in an image. Digital Image forgery can be broadly classified into two major domain categories: Active and passive approaches.

VIII. ACTIVE/ INTRUSIVE/NON-BLIND METHOD

It is concerned with data hiding where certain information inserted inside the digital image by the imaging device during image acquisition or before the distribution of the image to the public. The embedded data in the image is used to detect the source of such an image or to perceive an alteration in that image.

A. Digital signature:

Digital signature is one among the active method used for detecting image forgery or tampering. Demonstrating the authenticity of digital document using a sort of mathematical scheme is called as digital signature. In digital signature robust bits are extracted from the original image. Image Signing process contain following steps:

1. Decompose the image using parameterized wavelet feature.
2. Extract the SDS.
3. Cryptographically hash the extracted SDS, generate the crypto signature by the image senders private key.
4. Send the image and its associated crypto signature to the recipient.
5. Digital signature is simple and basic approach for digital image authentication.

B. Digital watermarking: Watermarking is also used for image forgery detection. Several watermarking techniques have been proposed. One uses a checksum schema in that it can add data into last most significant bit of pixels [8].

C. Passive / non-intrusive/ blind method

In disparity with active methods, passive or blind methods [9,10] of forgery detection take advantage of the traces left by the image processing operations performed in various phases while acquiring and storing the digital images. Such traces can be considered as a thumbprint of the image source device. Passive methods work in the absence of prior knowledge about the image, such as watermarks or signatures. There is nothing inserted in the image before its distribution. Passive methods make use of the available image only and a certainty that the manipulation operations alter the statistics of the image, which can help in its detection when the image is tampered with. Original images are supposed to have consistent characteristics, such as noise variation, lighting, shadows, and so on. Manipulating the contents of the image results in altering these characteristics, which make them inconsistent. Such inconsistencies in the statistics of the image can then be calculated in order to detect forgery. Passive methods are the only solution to decide the trustworthiness of a digital image when digital watermarks or signatures are not available. Instead, we doubt the integrity of that image, hence we need further analysis.

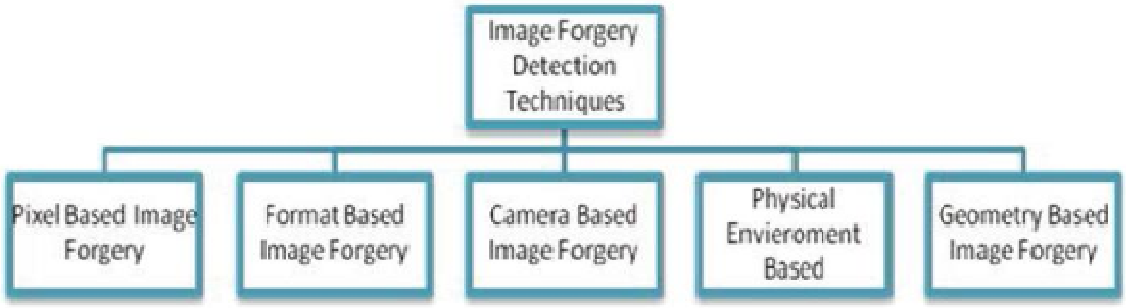


Figure 4: Types of digital image forgery techniques

A. Pixel based techniques focus on the digital image pixels which are the basic building blocks. These techniques work on different statistical anomalies which are introduced at the pixel level [11]. The working of these techniques is based on the alterations underlying statistics of the image.

B. Format based techniques works on the image format [12]. The most commonly used image format is JPEG and the format based forgery detection works mainly for the JPEG format. The blocking effect introduced by JPEG can be used to detect tampering in JPEG format. Manipulation of images causes the alteration of block artifact grids, especially in copy-move processing. There are three major categories JPEG Quantization, JPEG blocking and double JPEG which can detect image forgery even for compressed images.

C. Camera based techniques: Digital camera is the major device to take digital images. When a picture is taken, it involves a series of processing steps on the path from sensor to memory. White balancing, gamma correction, filtering and JPEG compression are the primary operations for the image to undergo [13].

D. Physical environment based techniques: The anomalies in the three dimensional interaction between the camera, light and the physical objects can be modelled through image forgery techniques based on physical

environment [14]. Such a picture may be made by grafting together individual pictures of each movie star. In this manner, it is frequently hard to exactly match the lighting effects under which each individual was initially captured. Here the background lighting difference can be used as the tampering evidence. The algorithms work on the basis of difference in the lighting environment.

E. Geometry based techniques: These techniques measure the world objects and their camera relative position. The two main geometry based techniques includes principal point and metric measurement [1]. The principle point for an image is located near the centre of the image. When the image object is transformed, the principle point also changes proportionally. Obtaining metric measurement from a single image is very useful in forensic settings where real-world measurements are required.

IX. GENERAL FRAMEWORK FOR FORGERY DETECTION

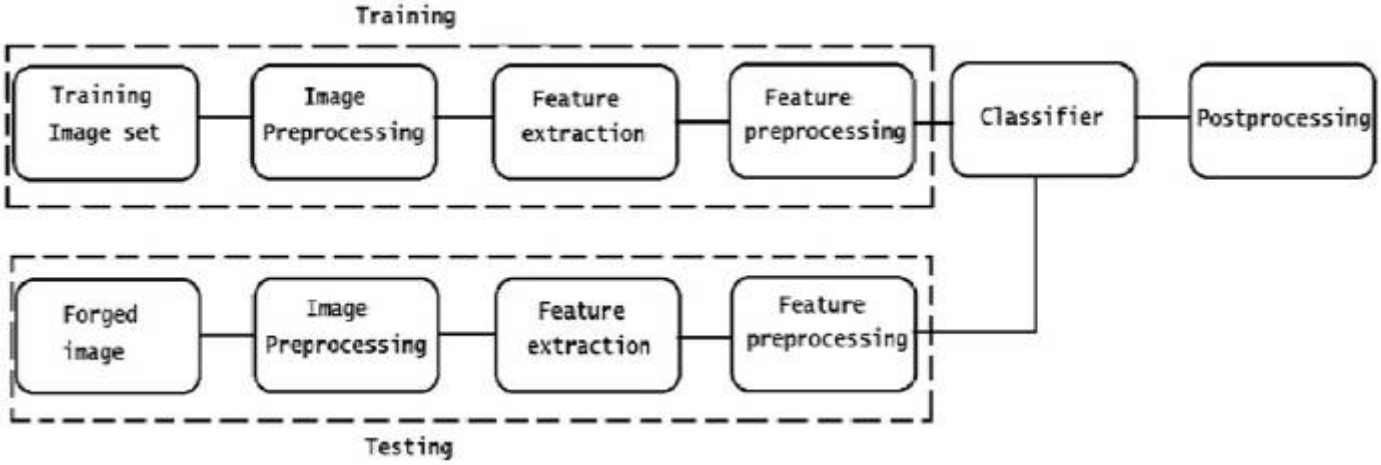


Figure 5: Framework for Image Forgery Detection

X. LITERATURE SURVEY OF COPY-MOVE TECHNIQUE

Detection algorithm for copy-move technique

Various algorithms are efficient in term of detecting forgery with less execution time but not robust in term of various attacks such as rotation, scaling, blurring, multiple copy-paste attack etc. The workflow used for finding forgery is shown in Figure 5.

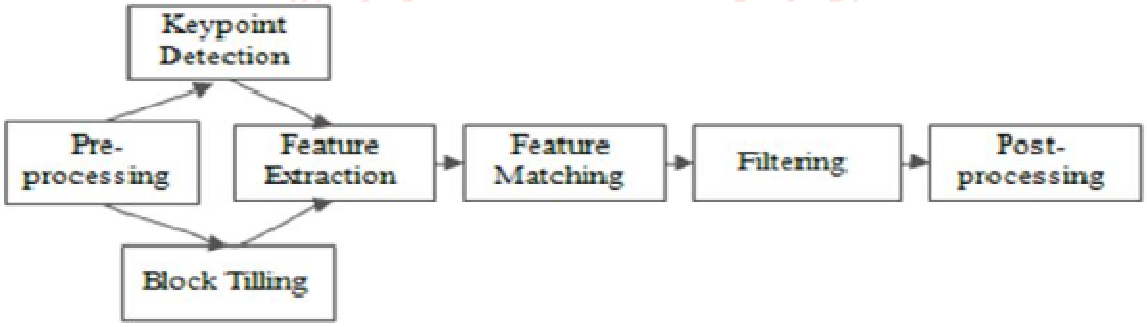


Figure 6: General block diagram of copy-move image forgery detection system.

Pre-processing: The purpose of pre-processing is enhancement in image data. Colour conversion is performed if there is requirement to convert colour image in gray scale image. Different pre-processing functions are applied like resizing input image, dimension reduction, filtering image with low-pass filter. In both block-based and key point based techniques, pre-processing can be applied.

Feature Extraction: In this step, feature vectors are extracted. If block based method is used, then image is divided in overlapping or non-overlapping blocks of fixed size. These blocks can be square or circular. In case of key point based methods, feature corresponding to key points are extracted.

Matching: After feature extraction, matching between feature vectors is performed for finding similar regions present in an image. Best-Bin-First searching procedure is used for identifying approximate nearest neighbour which helps in feature matching for key point based methods.

Filtering: Filtering procedures are used for reducing number of false matches.

Post-processing: The tampered regions are marked by colouring or mapping the region of matching blocks. Key-point based approach is displayed by line transformation between each matching point. Morphological operations refine the visualizations by using shapes such as contours, skeletons, convex hills

to connect matched pairs (fill the holes in marked regions) and remove outliers (isolated regions).

Block based Approaches

In block-based methods, input image is divided into fixed size overlapping or non overlapping blocks. Generally, Square blocks are used but some researchers also used circular blocks. Features are extracted from each block using several methods such as intensity-based, moment-based, dimensionality reduction-based, frequency-based etc. Feature vectors are obtained from feature extraction algorithms and are matched using block-based matching algorithms.

The block based feature extraction methods involve:

- Quantized Discrete Cosine Transform (DCT) coefficients of blocks matched to detect the tampered regions.
- Principal Component Analysis (PCA) to reduce the block feature dimensions.
- RGB colour components and direction information as block features.
- Calculation of 24 blur invariant moments as block features.
- Fourier-Mellin Transform (FMT) for block feature calculation.
- Gray average results of each block and sub-blocks used as block features.
- Zernike moments for block feature.
- Information entropy used as block feature.
- Various block-based matching algorithms used in literature are:
- Sorting: lexicographic sorting, KD-tree, radix sort
- Hash: counting bloom filters, locality-sensitive hashing
- Phase correlation
- Euclidean distance
- Others: sum of difference between DCT coefficients and sequential clustering

Key-point based Approaches

The key point based approaches are mainly reckoning on the extracting local interest points. These points are also known as key-points. Further, extracting the local points with high entropy without any image sub-blocking. The best key-points are able to identify distinct locations in an image areas are considered as efficient key points. Key-point based methods are computationally less complex but they do suffer from issues. Key-point based matching algorithms are divided into following categories:

- Nearest neighbour
- Clustering

To overcome the drawbacks of block-based and key-point based methods, both are fused together to make a hybrid method. The hybrid method helps in reducing the overall complexity of the method, which was due to the block matching step. In key-point based methods, segmentation can be performed before extracting key-points in order to extract key-points from the whole image.

XI. A SURVEY OF COPY-MOVE DETECTION TECHNIQUES:

Fridrich et al.[15] introduced a first method for identifying copy-move image forgery in 2003 and discussed several major requirements of the copy-move detection algorithm, including: allowing for an approximate match of small image segments; and having few false alarms and an acceptable processing time or complexity. They then proposed a detection algorithm based on block matching. In this method, the image is divided into overlapping blocks (16 x16), and DCT coefficients are used for feature extraction of these blocks. This method is taking too much computational time and not able to detect tampered region if attacks are applied on image like rotation and scaling.

Popescu et al.[16] initiated a technique for identifying duplicate image regions in 2004. In this method, authors applied PCA on fixed-size image of block size (16 x 16, 32 x 32), then computed the Eigen values and eigenvectors of each block. The duplicate regions are automatically detected by using lexicographical sorting. This algorithm is an efficient and robust technique for image forgery detection even if the image is compressed or noisy.

To combat computational complexity ***Langille and Gong [17]*** proposed use of k-dimensional tree which uses a method that searches for blocks with similar intensity patterns using matching techniques. The resulting algorithm has a complexity of O(NaNb) where Na is neighbourhood search size and Nb is the number of blocks. This method has reduced complexity as compared to the earlier methods.

Li et al.[18] proposed a copy-move forgery detection based on sorted neighborhood approach by using DWT and SVD in 2007. In this paper, authors utilized DWT and disintegrated into four sub-groups LL, HL, LH, HH which contains the approximation band, Horizontal component of image, Vertical component of image, Diagonal component of image respectively.

Ghorbani et al.[19] proposed a method to detect copy-move forgery based on DWT-DCT (QCD) in 2011. DCT is used for feature extraction from the approximation band which is divided into overlapping blocks of fixed size. DCT extracts feature vector from

each block. These row feature vectors are sorted in a matrix. After that DCT coefficients are decomposed for this quantization is performed using quantized table.

Zandi et al. [20] proposed an adaptive copy-move forgery detection (CMFD) approach in 2014. This approach can be employed for most of the block-based copy-move forgery detection. Different thresholds were adopted for various image contents. As it is expressed, a higher threshold should be selected for textured areas since less false matches occurs in such regions. This is because more distinct features make block matching more reliable. On the contrary, a low threshold is more appropriate for smooth regions. The standard deviation (SD) estimates the energy of high frequency coefficients of the blocks. The matching threshold can be adjusted proportional to the SD of the pair block's intensity. This relationship is almost linear. Thus, the adaptive threshold of a specific block was determined by its SD; therefore, the corresponding CMFD can detect duplications in both smooth and textured regions. In addition to reducing the potential matches, this method outperforms the LSH based methods in terms of true positive and false positive rates.

Lee et al.[21] in 2015 proposed a block-based method based on the histogram of oriented gradient in which the image is divided into overlapping blocks. HOG features are extracted from each block and Euclidean distance matching is performed. The method detects multiple instances of copy-move in a single image but it is not rotation and scale invariant

Zhou et al. [22] in 2016 designed the CMFD algorithm based on color information and its histograms. Most of the forgery detection methods convert a RGB image into a grey scale image, which discards the colour information of the image. To utilize the colour information, colour moments are used to cluster the blocks according to their colour similarity. While Neural Networks can have only a certain type of sigmoidal or radial basis function, CPPN can have a mixture of such functions. The method is not rotation invariant.

Huang et al. [23] developed copy move forgery detection using Scale Invariant Feature Transform (SIFT) technique in 2009. Firstly, the authors have used SIFT technique to find the duplicate region with scale as well as rotation. Further, Best Bin First search (BBF) techniques have been used for finding possible duplicate key-points. Additionally, nearest neighbour distance ratio(NNDR) is applied to increase the detection rate or accuracy. This technique is able to find key-points even if image is noisy or compressed.

Christlein et al.[24] performed a comprehensive evaluation of various kinds of CMFD approaches. An image database containing 48 base images was adopted, and the copy-move forgeries were carefully produced without leaving visually noticeable traces. Of all the features, Zernike features are the recommended choice due to its relatively small memory footprint.

Li J et al. [25] proposed one of the hybrid methods in which the key-points are extracted using the SIFT algorithm by first segmenting the test image into semantically independent patches using SLIC (Simple Linear Iterative Clustering) segmentation with no less than 100 patches so as to cover all the possible forged regions. K-nearest neighbour is used for matching the patches. The (Expectation-Maximization) EM-based algorithm is then used in order to refine the matching.

Ardizzone et al. [26] built the triangulation onto the extracted key-points. In the regions where no key-points are extracted, uniformly arbitrary points are added onto the boundary of the image which helps in subdividing the parts of the image into triangles that have no keypoints. The triangles are matched using two characteristics, the dominant and the angles and the areas in the triangle. They are matched using a Mean Vertex Descriptor (MVD). The method is two orders of magnitude faster than block-based methods. In the case of complex scenes, the high number of triangles influences the matching process resulting in worse performance.

Zhong J [27] explored the Radon odd radial harmonic Fourier moments method (RORHFM) to improve performance against various operations such as rotation, scaling, translation etc. RORHFM is applied with a circle template to extract the geometric inherent features. Pearson Correlation Coefficient is applied to analyse the geometric transform of cloned forgeries to calculate and classify the statistical data. The kernel representation is more complex in RORHFM, which leads to computational complexity because computational complexity and cost of the method is mainly dependent on kernel function.

The drawback of combining block-based methods and key-point based methods is that if the first one is unsuccessful at identifying the forgery and the image is too smooth to have enough key-points, then the fusion approach cannot give accurate results.

XII. LITERATURE SURVEY OF SPLICING DETECTION TECHNIQUES

Image splicing is another commonly used forgery operation in images. It is therefore necessary to detect image splicing. For splicing, copy-move based techniques cannot be used as those techniques are

based on finding a matching region in the image, whereas, in splicing, the forged region is copied from another image. Hence, the forged region will have different characteristics as compared with the rest of the image. The presence of abrupt changes between different regions that are combined and their backgrounds, provide valuable traces to detect splicing in the image under consideration. Splicing-based methods use a variety of features such as Bicoherence features, camera response function, DCT and DWT coefficients, invariant image moments, Weber local descriptors, etc.

Ng and Chang [28] suggested an image-splicing detection method based on the use of bicoherence magnitude features and phase features. Detection accuracy of 70% was obtained. Same authors later developed a model for detection of discontinuity caused by abrupt splicing using bi-coherence.

X. Wu and Z. Fang [29] proposed the image splicing detection method which uses illuminantcolor inconsistency to detect image splicing and to locate spliced area. The author suggests that the irregularity at the colour edge is significant evidence that the image has been tampered. Given color image is divided into many overlapping blocks. Based on the content of blocks a classifier is used to adaptively select illuminantcolor estimation algorithm. Illuminantcolor is estimated for each block, and the difference between the estimation and reference illuminantcolor is measured. If the difference is larger than a threshold, the corresponding block is labelled as spliced block. Considering the impact of image content on the illumination color estimation, a maximum likelihood classifier is used to adaptively select illuminant estimation algorithm.

Zhao, Wang, Li, and Li [30] model the adjacent coefficient difference array in two different domains, i.e. BDCT domain and DWT domain as an observation for a 2-D Markov model.

Markov features are one of the most effective features for splicing detection. The entire feature set is then divided randomly into two sets: one for training and other for testing. The training set finds the optimal hyperplane and the testing set is used to test the effectiveness of the method. The method has high complexity but provides better robustness to JPEG compression and median filtering as compared with methods available in the literature.

Bahrami et al. [31] discussed that in order to hide the traces of splicing, blurring is the commonly performed operation. So, the authors proposed Local blur-type features which are generated by partitioning the image into blocks using a Generalized Gaussian Distribution (GGD). Second, a classifier is formulated to classify the image blocks into out-of-focus or motion blur based on the proposed features. Then, splicing localization is performed. The drawback of this method is that a human decision is needed to indicate the spliced region based on some inconsistencies in the blur type and the semantics of the image. Such detection is robust to image resizing and spliced region boundary blurring and does not need camera information. However, our method can be applied to blurred images only.

Zhan et al. [32] in 2016 proposed the image splicing detection method based on PCA minimum eigenvalues. In this method, an image is segmented into pixel-centred overlapping image blocks. Each block is resampled by the self-similarity pixel strategy (SSS). Then, the local minimum eigenvalues (LME) of the sample matrix calculated by PCA are analysed. A threshold is set to separate the LMEs into two clusters. The threshold can be obtained by the frequency histogram. In the literature, some methods select a few reference blocks and approximate their illuminant. The reference blocks are compared with a suspicious block to find out the angular error between them. If this value is more than the threshold value, the corresponding block is said to be manipulated. Such methods rely largely on user's perception and interaction capabilities to choose the correct reference blocks. If the reference blocks are not chosen correctly, the performance of the methods is strongly compromised. This method is suitable for any input splicing forgery images with inconsistent irrelevant components. It can localize the tampered region on the pixel level. What's more, the minimum eigenvalue exists as a property that only relates to image itself. It can be available by direct calculation without the estimation procedure, which eliminates the estimation errors affected by estimation methods and further increases the detection precision.

Kaur M, Gupta S [33] proposed a method based on wavelet transform by using DWT and LBP. A Sharp transition is introduced by splicing operation in the form of lines, corners, edges, etc. Such sharp transitions are characterized by high frequency components. To detect such transitions, wavelet coefficients can be analysed in order to measure local sharpness or smoothness. Low level coefficients are obtained using Single level discrete wavelet transform. Then, local binary patterns are used to extract the texture of these [LL, LH, HL, HH] components. A histogram of these texture images is considered for effective training and testing of features. The concatenation of LBP histograms is performed and fed to the SVM classifier for training.

The method has low computational complexity and is invariant to monotonic illumination changes. But the performance of the method degrades when the size of the image is too small.

Li C [34] proposed another method in which the colour components are utilized and information pertaining to colour is obtained from blocks of images to construct quaternion. Then quaternion discrete cosine transform (QDCT) is applied and its coefficients related to the blocks of images are extracted. The expanded Markov features generated from the transition probability matrices in QDCT domain can capture inter-block correlation between its coefficients along with the intra-block QDCT coefficients. Finally, the distinction between authentic and spliced images is made using the feature vector obtained with Primal SVM as a classifier. The algorithm not only make use of color information of images, but also can yield but also can significantly lead to improving the tampering detection rate, with more than 92.38% accuracy compared with the state-of-the-art splicing detection methods tested on the same dataset. Because the tamper images are mostly color in real life, this new idea for image tamper detection research has a certain theoretical and more practical significance.

XIII. LITERATURE SURVEY OF RETOUCHING BASED DETECTION TECHNIQUES

Image retouching detection is carried out by trying to find the blurring, enhancements, colour changes and illumination changes in the forged image. Detection is easy if the original image is available however blind detection is challenging task. For this type of forgery two type of modification is done either global or local. Local modification is done usually in copy-move and in splicing forgery. Contrast enhancement that is carried out in case of retouching is done at global level and for detection of tampering these are investigated. For illumination and changes in contrast global modification is carried out.

M. C. Stamm and K. J. R. Liu [35] gave an algorithm that describes a method that does not only detect global enhancements but also suggests methods for histogram equalization. A similar model based on the probabilistic model of pixel values is detailed in ***[36]*** that approximate the detection of contrast enhancement. Histograms for entries that are most likely to occur with corresponding artifacts due to enhancement are identified. This technique provides very accurate results in case the enhancement is not standard.

Cao et al. [37] developed a method for detection of gamma correction for image forgery detection. Then technique is based on estimation of histogram characteristics that are calculated by patterns of the peak gap features. These features are discriminated by the pre-computed histogram for the gamma correction detection in images. Results propose that this technique is very effective for both global and local gamma correction modifications.

X. F. Li et al. [38] developed a technique for detection of retouching which is based on the Bi-Laplacian filtering. This technique looks for matching blocks on the basis of a KD tree for each block of the image. This technique works well on uncompressed images and compressed high-resolution images. Accuracy also depends on area of the tampered region for high-level compressed images.

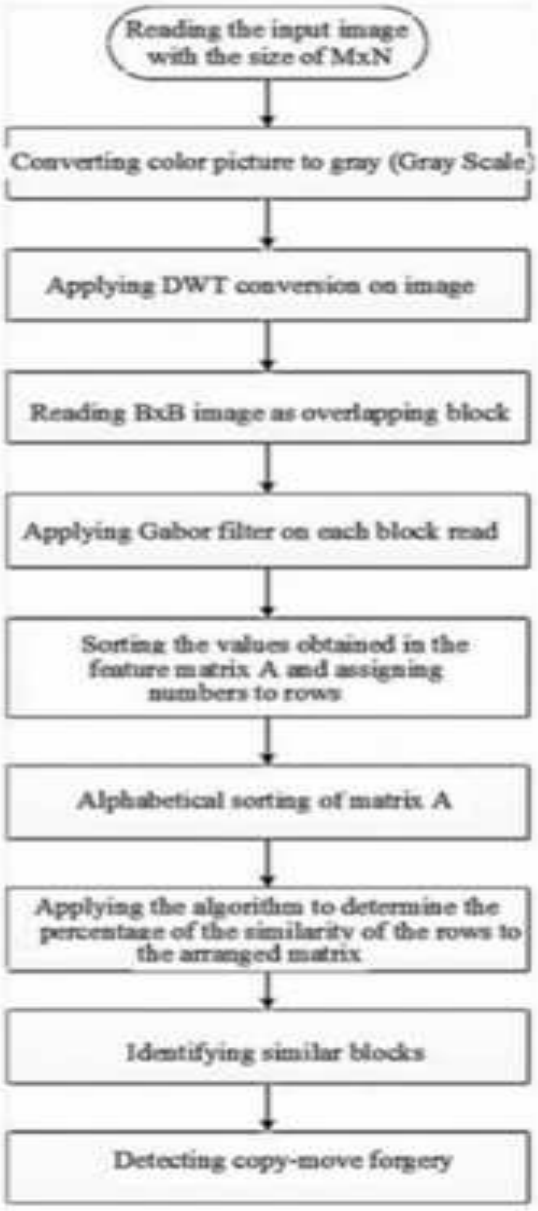
G. Cao et al. [39] developed two novel algorithms were developed to detect the contrast enhancement involved manipulations in digital images. It focuses on the detection of global contrast enhancement applied to JPEG-compressed images. The histogram peak/gap artifacts incurred by the JPEG compression and pixel value mappings are analysed theoretically, and distinguished by identifying the zero-height gap fingerprints. Another algorithm in same paper proposes to identify the composite image created by enforcing contrast adjustment on either one or both source regions. The positions of detected block wise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions. Both algorithms are very effective.

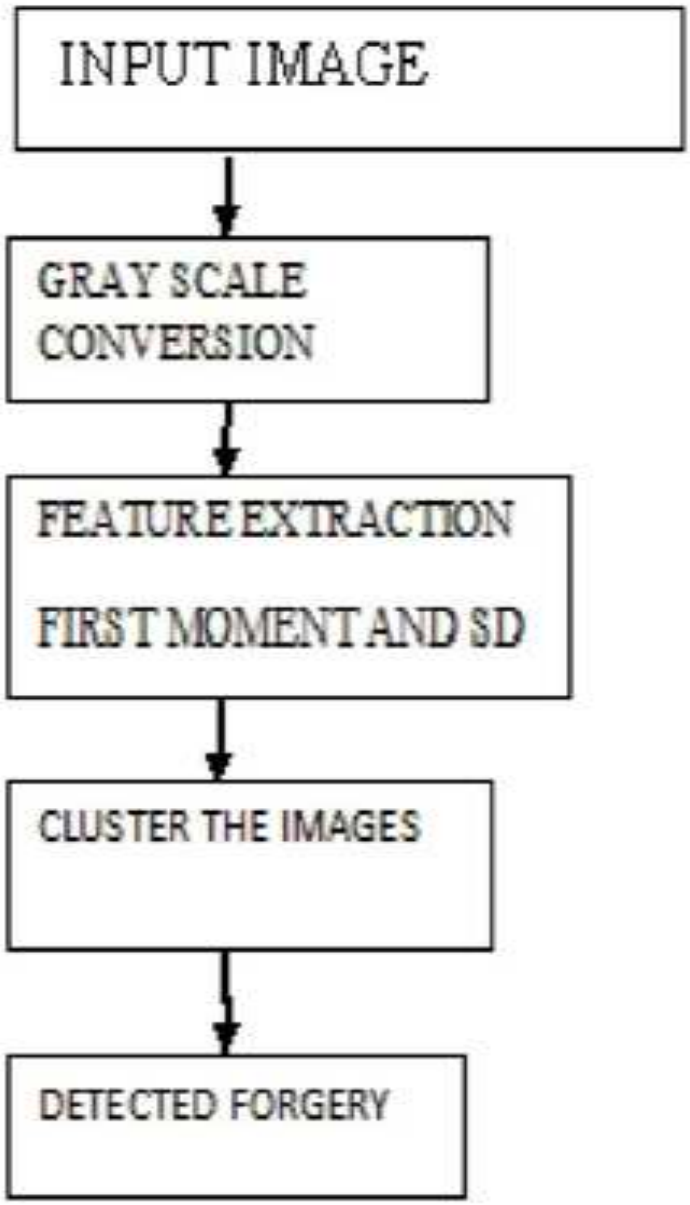
G. Chierchia [40] explored the techniques based on the photo-response non-uniformity (PRNU) that detect the absence of the camera PRNU. This algorithm detects image forgeries using sensor pattern noise. A Markov random field take decisions jointly on the whole image rather than individually for each pixel. This algorithm shows better performance and a wider practical application.

Number of methods have been proposed and discussed for retouching forgery. Limitation is that most of the methods work well if the image is greatly modified in comparison to the original image. Moreover, the human intervention required to interpret the result makes them non blind techniques.

XIV. PROPOSED METHODOLOGY

I will be taking two techniques of image forgery, one is Gabor Filter and the other one is BRICH, combining the algorithm of two and giving one hybrid algorithm as a result.





REFERENCES

[1] Farid H. Image forgery detection. IEEE Signal Process Mag. 2009; 26(2): 16–25.

[2] Reis G. Digital image integrity. San Jose, CA; 1999.

[3] Photo Tampering throughout history. Four and six Technologies, Inc. [Online]. [cited 2017 Aug 18]. Available from: http://pth izitru.com/

[4] Mhiripiri NA, Chari T. Media law, ethics, and policy in the digital age. United States of America: IGI Global; 2017.

[5] Salam A Thajeel and GhazaliSulong, A Survey of copy-move forgery detection techniques, Journal of Theoretical and Applied Information Technology, 2014, Vol. 70, No. 1, Pp. 25-35.

[6] Z. Zhang, Y. Ren, X. J. Ping, Z. Y. He and S. Z. Zhang, "A survey on passive-blind image forgery by doctor method detection", Proc. Seventh Int. Conf. on Machine Learning and Cybernetics, (2008), pp. 3463–3467.

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

[8] Doke KK, Patil SM. Digital signature scheme for image. International Journal of Computer Applications. 2012; 49(16): 1-6.

[9] Elwin JGR, Aditya TS, Shankar SM. Survey on passive methods of image tampering detection. Proceedings of the International Conference on Communication and Computational Intelligence; 2010 Dec 27–29; Perundurai, Erode: Kongu Engineering College; 2003. p. 431– 436.

[10] Qazi T, Hayat K, Khan SU, Madani SA, Khan IA, Kolodziej J, Li H, Lin W, Yow KC, et al. Survey on blind image forgery detection. IET Image Proc. 2013; 7(7): 660–670.

[11] Pradyumna Deshpande and PrashastiKanikar, Pixel Based Digital Image Forgery Detection

Techniques, International Journal of Engineering Research and Applications, 2012, Vol. 2, Issue 3, Pp. 539-543.

[12] Harpreet Kaur, Kamalijit Kaur, A Brief Survey of Different Techniques for Detecting Copy Move Forgery, International Journal of Advanced Research in Computer Science and Software Engineering, 2015, Vol. 5, Issue. 4.

[13] Wei Wang et al, A Survey of Passive Image Tampering Detection, Springer, 2009, Pp. 308 322.

[14] Akanksha Namdeo1and Anish Vishwakarma, A Survey on Copy Move Image Forgery Detection Using Wavelet Transform, International Journal of Science and Research, 2013, Vol. 4, Issue 3, Pp. 876-878.

[15] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy move forgery in digital images," Proceedings of the Digital Forensic Research Workshop, pp. 5-8, Aug. 2003.

[16] A. C. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep., TR2004-515, 2004.

[17] 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.

[18] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp. 1750-1753.

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

[20] Zandi M, Mahmoudi-Aznaveh A, Mansouri A. Adaptive matching for copy move Forgery detection. In: Proceedings of 2014 IEEE International Workshop on Information Forensics and Security; 2014 Dec 3–5; Atlanta, GA, USA. Piscataway: IEEE; 2014. p. 119–24.

[21] Lee J-C, Chang C-P, Chen W-K. Detection of copy-move image forgery using histogram of orientated gradients. InfSci (NY). 2015; 321: 250–262.

[22] Zhou H, Shen Y, Zhu X, Liu B, Fu Z, Fan N. Digital image modification detection using color information and its histograms. Forensic Sci Int. 2016; 266: 379–388.

[23] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-6, Dec. 2009.

[24] Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copymove forgery detection approaches. IEEE Trans InfForen Sec 2012; 7(6): 1841–54.

[25] Li J, Li X, Yang B, Sun X. Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur. 2015; 10(3): 507–518.

[26] Ardizzone E, Bruno A, Mazzola G. Copy-move forgery detection by matching triangles of keypoints. IEEE Trans Inf Forensics Secur. 2015; 10(10): 2084–2094.

[27] Zhong J, Gan Y, Xie S. Radon odd radial harmonic Fourier moments in detecting cloned forgery image. Chaos Solitons Fractals. 2016; 89: 115–129.

[28] T. Ng and S. Chang, "A model for image splicing", Proc. of IEEE International conference on image processing (ICIP), (2004), pp. 1169–72.

[29] X. Wu and Z. Fang, "Image Splicing Detection Using Illuminant Color Inconsistency", International Conference on Multimedia Information Networking and Security (MINES), (2011), pp. 600-603.

[30] Zhao X, Wang S, Li S, Li J. Passive image splicing detection by a 2-D Noncausal Markov Model. IEEE Trans Circuits Syst Video Technol. 2015; 25(2): 185–199.

[31] Bahrami K, Kot AC, Li L, Li H. Blurred image splicing localization by exposing blur type inconsistency. IEEE Trans Inf Forensics Secur. 2015; 10(5): 999–1009.

[32] Zhan L, Zhu Y, Mo Z. An image splicing detection method based on PCA minimum eigenvalues. J Inf Hiding Multimed Signal Process. 2016; 7(3): 610–619.

[33] Kaur M, Gupta S. A passive blind approach for image splicing detection based on DWT and LBP histograms. Int SympSecurComputCommun. 2016: 318–327.

[34] Li C. Image splicing detection based on Markov features in QDCT domain. Neurocomputing. 2017; 228: 29–36.

[35] M. C. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images", Proc. 15th IEEE Int. Conf. Image Processing 2008, (ICIP'2008), (2008), pp. 3112–3115.

[36] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast. Enhancement mapping", Proc. IEEE Int. Conf. Acoustics speech and signal processing (ICASSP), (2010), pp. 1698-1701.

[37] G. Cao, Y. Zhao and R. Ni, "Forensic estimation of gamma correction in digital images", Proc. 17th IEEE Int. Conf. on Image Processing, (ICIP'2010), (2010), pp. 2097–2100.

[38] X. F. Li, X. J. Shen and H. P. Chen, "Blind identification algorithm for the retouched images based on bi-Laplacian", Comput. Appl., vol. 31, (2011), pp. 239–242.

[39] G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, (2014), pp. 515-525.

[40] G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection", Information Forensics and Security, IEEE Transactions, vol. 9, no. 4, (2014), pp. 554-567.