Blind Approach for Digital Image Forgery Detection

Tulsi Thakur
M.Tech Department of
Computer Technology
YCCE, Nagpur
Maharashtra, India

Kavita Singh
Head & Associate Professor
Department of Computer
Technology
YCCE, Nagpur
Maharashtra, India

Arun Yadav
Tata Consultancy Services
Mihan, Nagpur
Maharashtra, India

ABSTRACT

In the digital era of where everyone is exposed to a visual imagery in very large extent. Digital images are very convincible way to share information. Due to the rapidly growing field of digital image acquirement and editing software that are impressive as well sophisticated with many advanced features. Manipulation with features of digital image can perform easily with the help of editing tools, which are cost effectively available online or offline and do not leave any visible footprint of tampering with an image. Forgery with the digital image is an unavoidable problem concern with the image authenticity and also with image integrity. Which raising a compulsion to take an immediate action on the forgery of the digital image to verify the authenticity and maintain the integrity. To encounter the problem of authenticity of digital image, this paper proposed a methodology for detection of image splicing forgery using the blind approach *i.e.,* passive method to detect the spliced region in the digital image. In passive approach, there is no provision for the pre-introduction of the watermark and pre-embedded digital signature during the time of image obtainment. This paper mainly concern with the image splicing forgery and it initiate with the DWT (Discrete Wavelet Transform) method, which will decompose the image into sub images and obtain coefficient for each sub image. After that for feature extraction we will use SURF (Speed-Up Robust Features) and finally SVM (Support Vector Machine) will perform classification for splicing forgery detection in digital image.

Keywords

Digital image forgery, Tampering detection technique, Copy-move forgery, Splicing forgery, Image retouching, DWT, SVM, SURF

1. INTRODUCTION

In the digital age, where the digital image provides the convincible and easiest way to convey any message more impactful than that of description. Digital Image has accomplished a prestige as an undeniable testimony. Spiraling fraudulent activities in an uncontrollable manner raised the question on the originality of the digital image and made harder to trust the legitimacy of the digital images as the tampering with the digital image can carried out with ease, due to availability of digital image manipulation software online or offline. This provides liberty to a naïve person to manipulate the digital image effortlessly without any technical knowledge about the domain. Digital image forgery can perform by manipulating features of the digital image, which leads to the changes in visual message of imagery. The digital image trustworthiness is consequential in many social areas. To conquer, there is compulsion to take an immediate action on tamparing with the digital image to certify the authenticity and maintain the integrity of digital image to preserve the genuineness of an image.

Nevertheless, the dilemma concerned with the authenticity of digital image appeal for the verification of legitimacy of the digital image in diverse applications. Integrity and authenticity of the digital image play a prime role in courtrooms as evidence, even in journalism, magazines, social media rely on the digital images as well as the medical field also believe in the digital imagery for reports. The digital image usage do not bound to this end, even the educational institutes are having faith in digital image. This invites the forgery detection mechanism to identify and certify the digital image as trustworthy.

From the above mentioned usage of the digital image, it is undeniable that the role of a digital image has arisen as need of the time in every field of life. This made an urgency to develop a mechanism to verify and certify the genuineness of an image.

The rest of the paper is systematized as follows. Introduction of the paper has given in Section I and the Section II will discuss about the types of digital image forgery and the next Section III is given for study over various types of digital image forgery detection techniques. Furthermore, Section IV and V conferred review on various proposed techniques for the detection of digital image forgery in the context of the three mentioned forgeries, along with the comparison. At the end, conclusion is given in the Section VI.

2. TYPES OF IMAGE FORGERY DETECTION TECHNIQUE

In this following section, the paper explains comprehensive concept regarding the types of image forgery detection techniques. The main goal of image forgery detection mechanism to authenticate the digital image; this is a facility to discover the falsification in the digital image and maintain the integrity of an image. Classification of the image forgery detection technique is mainly splits into two separate approaches, *viz;* active approach and passive approach.

2.1 Active Approach

In active approach, the digital image depends on some additional pre-inserted information such as digital watermark insertion or attaching digital signature on the image at the time of image recording. However, during exercising it would create a boundary against the active approach. Nevertheless, many cameras do not outfitted with these characteristics that results failure of active approach.

2.1.1 Digital Watermark

A digital watermark is sort of digital marker which embeds to image at the image acquisition process by well-equipped camera. Digital watermarking is a technology that grant user to embed digital information, which used to apply on the digital document like image to uniquely identify ownership or originator of the digital image. It is an active approach to preserve the attack on the genuineness of the digital image.

2.1.2 Digital Signature

A digital signature is a cryptographic phenomenon that is a mathematical term and it is process which inserts the digital signature on the digital document like an image to provide assurance for no alteration employed on the digital image. It is one of the active approaches that verify the authenticity of digital image.

2.2 Passive Approach (Blind Approach)

A passive or blind approach recently gained significant attention in field of the image forgery detection from the many researchers as it work in the absence of hidden data mounted with the digital image. These approaches authenticate the digital image by investigating the changes occurred in characteristics of an image during the tampering process. Although, there is a hypothesis which consider that no visible impression left by the image forgery techniques while performing tampering with an image. Many existent methods localize forged region in the digital image by identifying forgery and traces left by tampering techniques.

Moreover, passive approach is sub-divided into several categories based on the tampering perform on the digital images. Namely, categories are copy-move, image splicing and image retouching. Figure 4 shows the classification of the image forgery detection techniques.

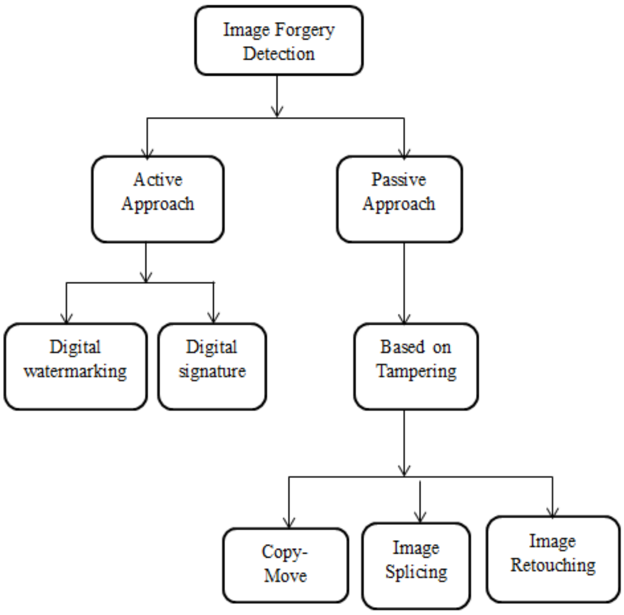


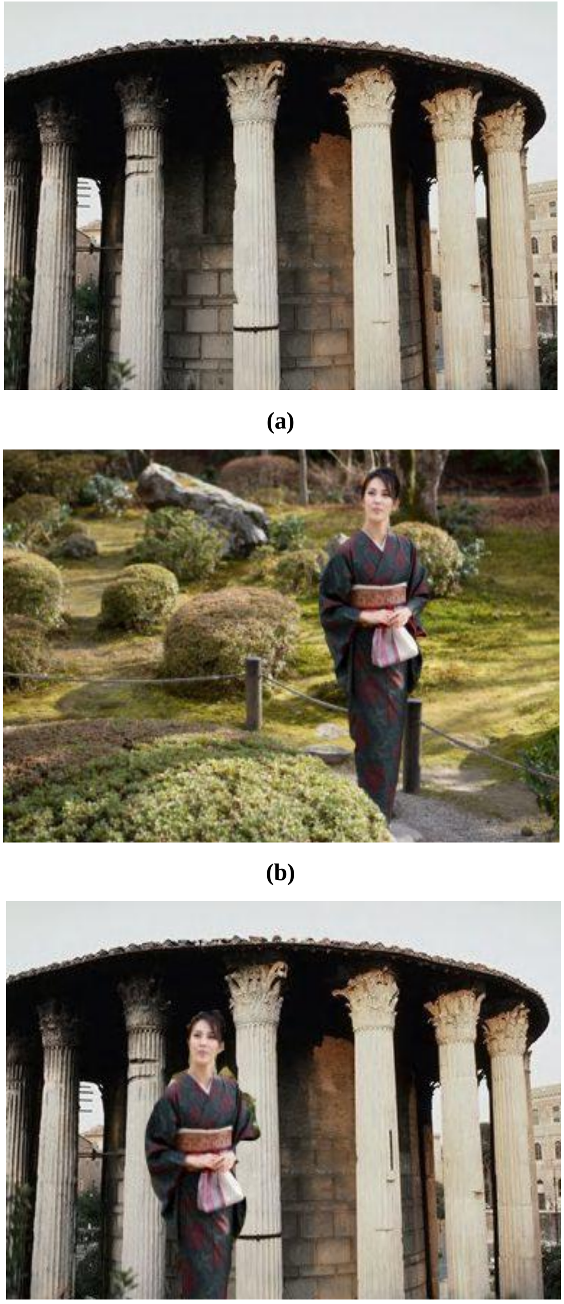
Fig. 4 Classification of Image Forgery Detection Techniques [3]

3. TYPES OF DIGITAL IMAGE FORGERY

In this section, discussion on the types of the digital image forgery will accomplish. Digital image can be termed as forged image when features of an image will manipulate using image editing tools *viz;* Photoshop, Picasa. The digital image forgery can be classified namely in four distinct digital image forgeries such as Copy-Move Forgery, Image Splicing Forgery, Image Retouching and Image morphing.

3.1 Image Splicing

Image splicing forgery is phenomenon which simply cut and pastes the portion of an image from the same or different source images to make spliced image. Image splicing forgery changes visual information drastically than other forgeries [1].



(a)

(b)

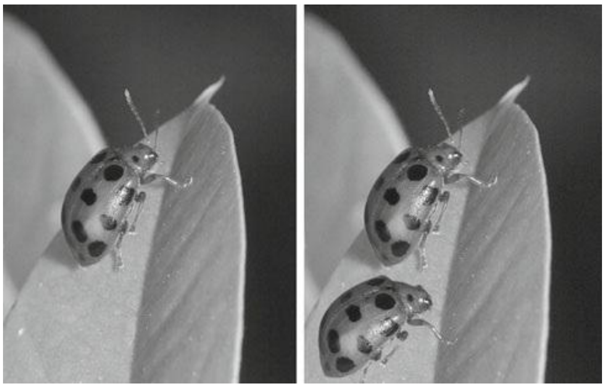
(c)

Fig. 1 Example of Image Splicing Forgery (a) Original image of woman standing in a garden (b) Original image of pillars and (c) Tampered image with woman and pillar combined (Source image is from CASIA TIDE v1.0 Dataset [23])

Image splicing is generally used mechanism in image forgery that simply merges two separate images to generate a spliced image. Image splicing forgery also acknowledge as Image Compositing forgery as it composites two distinct image piece and produce an image as presented in the figure 1. Where figure 1(a) and figure 1(b) are illustrating the original image and the figure 1(c) is describing the doctored image (i.e. spliced image). In the figure 1(c), two separate image's parts fused to create a composite image that results to transformation appeared to original image and it changes the whole meaning of the original image's visual information or features. In while combining two separate images taken in different time and place can cause to imbalanced in the original image and doctored image, this mismatch can be used as parameter for detecting image splicing forgery.

3.2 Copy-Move Forgery

Copy-move forgery is widespread image temparing technique that used to manipulate the digital image content. It is a type of image forgery where a region is copied and pasted on another in the same image frame either to camouflage or to clone the object in the image multiple times. During temparing the digital image by directly copying a region or a part of the digital image and pasting it into the same image frame on another region [1].



(a) *(b)*

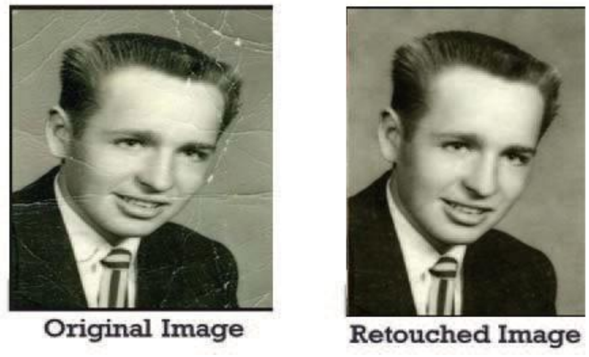
Fig. 2 Example of Copy-Move Forgery (a) Original Image (b) Tampered Image [17].

Copy-move forgery is also recognized as cloning forgery, as in copy-move forgery it clones an entity many times in the similar image frame, as displayed in the figure 2. The figure 2(a) illustrates the original image and figure 2(b) is as tampered image. From the figure 2(a), it can be observed that original image contained an insect. On the contrary, the figure 2(b) has been cloned which describe the tampered image presented two insects, where the entity of the same image is cloned in the similar image frame.

3.3 Image Retouching

The image retouching forgery is an art and science of image transformation where the visual imagery contents enhanced by performing several transformations using the available photo editing software [3]. Image retouching is mostly used technique by all dominant photographers to enhance the feature of the digital image as well as to restore the features of the digital image. Image retouching is a method that applied for beautification of characteristics of an image and preserves the originality of the digital image to give it natural visual imagery.

The figure 3 gives an example of image retouching, where the figure 3(a) shows an original image and figure 3(b) shows a retouched version of an original digital image. To make figure 3(a) more attractive, beautification filter has been employed on the digital original image. In journalism and photography world, Image retouching is extensively used by many magazines' editors and photographers to beautify elements of the digital image to make it look appealing.

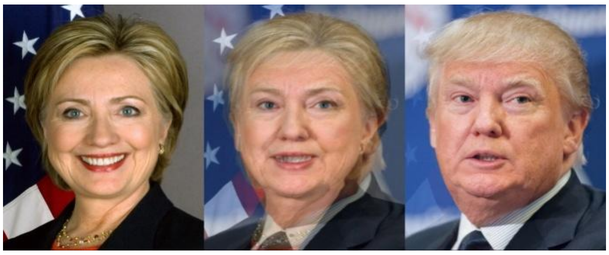


(a) **(b)**

Fig. 3 Example of Image Retouching (a) Original Image (b) Tampered Image [2].

3.4 Image Morphing

Morphing encompasses the process of metamorphosis for transformation of one digital image into another image through continuous treatment on an image. Morphing joins both image features viz; geometry and color of elements from many distinct images. Image morphing is generally used to create an intermediate between two different styles by designer in modern digital font design.



(a) **(b)** **(c)**

Fig. 4 Example of Image Morphing (a) Original image of Hillary Clinton (b) Morphed image (c) Original image of Donald Trump

Oftentimes, morphing employed to present one person image turning into another person image using continuous technological sequences of transformation. In left, figure 4 shows an example of image morphing, where figure 4(a) depicts the original image of Hillary Clinton, whereas figure 4(b) shows a morphed image of left side and right side image of Hillary Clinton and Donald Trump respectively, and in right, the original image of Donald Trump shows in figure 4(c). Image morphing can create an issue for digital image, as in this image of one person can turn into another person which raise question an image authenticity.

In spite of copy-move and image retouching, image splicing forgery challenges the digital world more sensibly as it alter the visual image information with more impact than other mentioned forgery techniques *viz;* copy-move forgery and image retouching. Although, image retouching contains many image beautification transformations such as color enhancement, skin retouching, photo cartooning, photo restoration, illumination changes *etc.* Image retouching does not reflect more changes in visual scenery. On the other hand, copy-move forgery displays multiple clone of an object in same scenery of digital image. In addition, Morphing influences digital world more gracefully as it can depict image of one person as another person.

In previous section, it has been realized that digital image forgery generated problematic situation for images as images employ in various areas like journalism, research, medical, educational as well as financial. Digital images are used in day today life scenario for several usages. Tampering with digital images induces question on the credibility of digital image that call for research on image forgery detection mechanism to authenticate the digital image trustworthiness. Many researchers have presented several mechanisms to overcome image forgery detection in different scenario.

In next section, this paper discusses on the proposed blind approaches by many researchers for the detection of image forgery with respect to the tampering type and changes occurred in an image.

4. RELATED WORK

This section initiate with the discussion on generalized steps involve in technique for forgery detection in an image. Further after, it continue with discussion on several proposed blind (passive) approach by many researchers for the detection of forgery in the digital image to conquer the problem of genuineness of image as well as to prove authenticity of digital images.

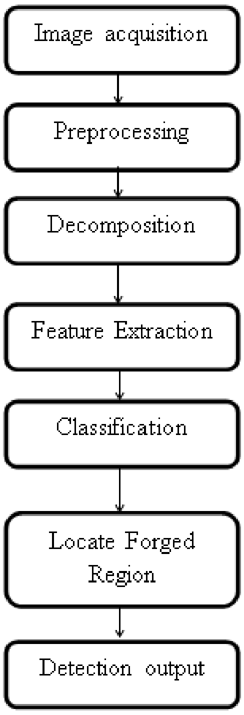


Fig. 5 General Flow of Image Forgery Detection

The generalize flow structure of the digital image forgery detection mechanism involve Image acquisition step that take an image as input to the technique followed by Preprocessing step. Preprocessing step perform conversion from one color space to required color space as well for noise removal. Next step is Decomposition that fundamentally segments the image into several image blocks to perform extraction of features from those decomposed image blocks in Feature Extraction step of image forgery detection mechanism. Intermediate step of the mechanism *i.e.,* Classification step which accomplish comparison to classify the extracted features of blocks that followed by localization of the tampered region of an image. In the last, Detection of forgery in image will be declared.

Figure 5 shows the general flow structure of the detection mechanism of image forgery with each specified step. Presented steps give details on blind approach based on tampering that also involve their assigned task.

In recent times, several researches have been done on the image forgery detection by many research scholars to preserve the legitimacy of the digital image. Most of the researchers used the Blind approach techniques for identification of forgery type and the localization of tampered region of image. By considering, blind approach does not depend on the prior information which has been inserted on the image at time of image acquisition for detection of tampering with an image.

Review on the digital image forgery detection methods based on the different methods presented by V. P. Nampoothiri *et. al.,* in [1] as well yields about the requirement of image tampering detection mechanism in the digital age. Paper [1] also performed comparative analysis with various techniques for tampering detection in digital image. In paper [2], Charmil Nitin Bharti *et. al.,* come up with the classification of digital image forgery methods and disclosed the passive image forgery detection techniques. Shwetha B *et. al.,* in [20] analyzed the various types of digital image forgery along with their detection method and classified them into the camera-based techniques, physical environment-based technique, format based techniques, pixel-based techniques and geometry-based techniques.

Most of the researchers frequently used Discrete Wavelet Transform (DWT) method for detection of image forgery. In many copy-move forgery detection mechanisms, DWT has been employed for image decomposition that assisted in minimization of size required for digital image at each level and it segments the image into four sub-images at each level namely LL, LH, HL and HH. The DWT method applied in [10] by Z. Zhang *et. al.,* to encounter transient changes occurred in spatial or frequency domain to calculate the statistical dissimilarity of an image. Although, in [14] Mohammad Farukh Hashmi *et. al.,* presented a technique that has been used DWT decomposition method to acquire LL sub-image. As LL part consider as approximate image that contains the most of the information of the processed digital image. In addition, one more researcher Preeti Yadav presented an algorithm in [7], where DWT transform implemented on image to attain the sub-divided overlapping blocks that were lexicographically sorted for obtainment of duplicated image blocks which resulted to identify the copy-move forgery in the digital image. The proposed algorithm in [7] initiated the detection of copy-move forgery with LL sub-image *i.e.,* the lowest level image representation. Moreover, Abhishek Kashyap *et. al.,* in the paper [8] as well as Pradyumna Deshpande *et. al.,* in [12] exercised DWT transform in their proposed mechanism for image forgery detection. In [12] researchers do not take scale and rotation parameter in consideration for copy-move image forgery identification. And in paper [21] Guohui LiI *et. al.,* illustrated a blind approach for image forensic to detect duplicated region in an image using DWT method to obtain the lowfrequency component of the digital image which further processed by sliding window operation of moving pixel.

For detecting image forgery Discrete Cosine Transform (DCT) transform has been generally applied method for dimensionality reduction of an image. Shinfeng D. Lin *et. al.,* in [4] discussed the format-based technique that essentially targeted on JPEG format as JPEG is the foremost used format of an image and ultimately proposed technique detected two image forgeries *viz;* copy-move and splicing forgery. The analysis performed over double compression effect in spatial and where coefficients' of DCT performed analysis on double compressed JPEG digital image. However, in [3] Amani A. Alahmadi *et. al.,* explained a passive approach based image splicing forgery detection technique that has been implemented DCT transform to extract DCT coefficients from the chrominance component (Cb or Cr) that was divided into 16×16 overlapping blocks as DCT decomposes the digital image into overlapping sub-blocks. In addition, Local Binary Pattern (LBP), codes estimated for those blocks and calculation of standard deviation for respective coefficients has been performed that were used as features. Author assured accuracies 97%, 97.5% and 96.6% over datasets CASIA TIDE v1.0 [23], CASIA TIDE v2.0 [24] and Columbia dataset [25] respectively for image splicing detection.

Whereas, Zhen Zhang *et. al.,* [10] come up with the concept of moment features that has been extracted from Multi-Size Block Discrete Cosine Transform (MBDCT), which reflected the differences appeared during image splicing in the local frequency and coefficients of MBDCT presented the changed of frequency distribution. Likewise, many research scholars have been proposed edge information dependent methodology for image forgery detection that helped effectively in both image forgery types *i.e.,* copy-move and splicing in the digital image. Abhishek Kashyap *et. al.,* in [8], also observed an outline analysis using DCT Transform. Analysis performed against the Object's outline with respect to smoothness and sharpness of edges in mentioned technique. Moreover, the paper [16] presented by Reza Moradi Rad *et. al.,* tossed an idea regarding edge block estimation using DCT transform and canny method. Canny edge detection method was employed on digital image to catch edge blocks conceptually that was looking for edges of object in an image. The objective behind the detection of edge block to obtain objects with inconsistent boundary edges for forgery detection in an image. Likewise, Varsha Sharma *et. al.,* in [19], proposed an approach that basically used DCT to decompose an image into several overlapping blocks and blocks were processed for coefficient extraction from the image blocks to present distribution of frequency in blocks and proposed method shown robustness against the added Gaussian noise and JPEG compression along with geometric parameter like scaling and rotation.

Features have prime importance in image forgery detection processing and useful feature extraction from the digital image is the process that labeled as Feature Extraction process. To detect tampered region in an image, it is essential to extract specific artifacts and hence many researcher pay attention on selecting correct feature extraction mechanism. Researcher mainly considered a key-point-based feature extractor and descriptors for identification of tampering in an image such as Scale-invariant Feature Transform (SIFT) [14-15], Singular Value Decomposition (SVD)[21-22], Speed-Up Robust Features (SURF)[4] and Mirror Invariance Feature Transform (MIFT)[17] that are robust against the scaling and rotation. Additionally, SIFT is also invariant to illumination and noise.

Rajeev Rajkumar *et. al.,* in [15] as well Mohammad Farukh Hashmi *et. al.,* in [14] employed SIFT feature extractor which extract artifacts those were robust against the scaling geometric parameter. In [15], proposed a method for copy-move forgery detection mechanism in which SIFT has been employed for extraction of helpful features for identification of duplicated region along with cluster formation for matching of keypoint artifact based on similarity between two region in the digital image. Likewise, in [14] Mohammad Farukh Hashmi applied SIFT feature extractor on lowest-level frequency *i.e.,* LL coefficient that contained approximately all information of an image. SIFT used to extract the key features and by comparing features based on similarity between several distinct feature descriptors and localized the cloned region of an image based on the extra ted artifacts.

Nevertheless, MIFT feature extractor introduced by Kalyani Khuspe *et. al.,* in [17] with a novel methodology for identification of Copy-Move digital image forgery by applying keypoint-based MIFT features that did not only referred the attributes of SIFT feature extractor, but also it was robust against the mirror reflection transformations. Proposed method also performed clustering on the set of images afterwards extraction of the MIFT features executed and codebook has been generated by the centroid of each cluster and codebook employed for intercommunication between recipient and transmitter. Although, SURF is next version of SIFT feature extractor as well as SURF is fast over SIFT. Key-based feature extractor SURF neglected by researchers and very few researchers employed SURF to deal with image forgery detection and Shinfeng D. Lin *et. al.,* in paper [4] practiced SURF for extraction of features that were helpful in forged region detection as well as it shown robustness against rotation and scaling.

Moreover, SVD method is feature extraction technique that applied by many researchers for image forgery detection such as copy-move forgery detection. SVD encompasses many invariant properties such as invariant to scaling, invariant to rotation and contains features stability. In [21] Guohui LiI *et. al.,* and XiaoBing Kang *et. al.,* in the paper [22] presented mechanisms that employed SVD for feature extraction. In [21], SVD technique has been employed on LL coefficient of DWT for extraction of steady artifacts of an image that used for identification of duplicated region. Likewise, paper [22] presented a framework for identifying the location of tampered region in an image by employing SVD feature extractor. SVD extracted algebraic as well geometric parameter invariant artifacts that has been shown robustness against many attacks suck as Gaussian white noise, JPEG compression, contamination, *etc.*

Additionally, in [5] Yu Fan *et. al.,* discussed a methodology that was based on the inconsistency of the illuminant color in the object areas of lightning effect in the spliced image that employed for identification of the digital image forgery. Segmentation has been performed on the digital image in some horizontal and vertical bands and then estimation of the illuminant of each band has been performed by applying the generalized grey-world algorithms [5]. The only problem with the proposed method in [5] that it has necessity of human intervention for suspicious annotation of an object to finalize the detection result.

Moreover, a new technique has been introduced by S. Devi Mahalakshmi *et. al.*, in [6], which discussed a methodology based on codebook. Generation of Codebook has been performed from the set of image features to extract the geometric manipulations those have been occurred in the received digital image. Before transmission, image hash based on bag of visual words inserted as a digital signature to an image. Forensic image hash has been compared at the destination end, to identify the tampering done with the received image. To deal with highly textured and contrasted tampered pattern that has been encoded spatial distribution of image features. There was requirement of the source image i.e., authenticate image for comparison between forged and original image to identify and localized the spliced region in an image, though it performed well with the copy-move forgery detection.

However, Tae Hee Park *et. al.*, tossed an idea regarding an image splicing detection by employing the characteristic function moments for the inter-scale co-occurrence matrix in the wavelet domain with the help of luminance components of an image in [9]. Generation of high-order characteristic function moments of the two-dimensional joint density function performed by applying the inter-scale co-concurrent matrices for localization of image splicing forgery in the digital image. Precision has been estimated with 96.2 % for the Columbia image splicing detection evaluation dataset [25]. Whereas, Wei Wang *et. al.*, presented a technique in [11] that dealt with a passive color image splicing forgery and analyzed chroma components of image to determine gray level co-occurrence matrix (GLCM) of threshold edge images of image chroma components and edge images were analyzed by subtracting horizontal, vertical, main and minor diagonal pixel values from current pixel values, respectively and then threshold with a predefined threshold T. In addition, the GLCMs of edge images along the four directions serve as useful features for identification of image splicing in the digital image. It has been observed, features of Cb (or Cr) components were more effective than Y component in [11] as same as in paper [3] the chroma component Cb and Cr were more effective than the Y component. Although, in paper [3] Meera Mary Isaaca et. al., presented the technique for copy-move along with splicing forgery detection in digital image. In the paper [13], Gabor Wavelet Transform (GWT) has been employed to the chroma component of the received image at different scales and rotation. Further, obtainment of Local Phase Quantization (LPQ) values were calculated for each of the gabor sub-images by applying LPQ operator. Feature vector has been produced by extracted LPQ values from distinct sub-bands of gabor wavelet.

5. COMPARATIVE ANALYSIS

An overview of all image forgery detection techniques given in section 4 with summarized analysis. All mentioned image tampering detection mechanism were able to localized and detect the distinct varieties of digital image tampering in addition with other post-processing like blurring, rotation, scaling, *etc.* Analysis can perform on digital image forgery as well as detection techniques of image forgery in conjunction with comparison with respect to their properties and different artifacts of the digital image. Table 1 summarizes several distinct digital image forgery detection mechanisms along with their domain of detection, employed techniques, their merits as well as their limitations.

Table 1. Comparative analysis of different image forgery detection techniques

Sr.no	Paper	Technique	Detection Domain	Advantage	Limitation
1	Splicing Image Forgery Detection Based on DCT and Local Binary Pattern [3]	LBP, DCT, SVM	Image Splicing Forgery	Attained 97% accuracy with chrominance color space	Less accurate in gray and color channel
2	An Integrated Technique for Splicing and Copy-move Forgery Image Detection [4]	DCT, SURF	Spliced Image and Copy-move Forgery	Successfully localized multiple forged region in the same image	Restricted to specific image format like JPEG
3	Image Splicing Detection with Local Illumination Estimation [5]	Local Illumination Estimation, color inconstancy.	Spliced Image	robust over two datasets with good accuracy	Need of human intervention
4	A Forensic Method for Detecting Image Forgery [6]	Code-book, Hash	Spliced image and copy-move image forgery	Generated less complex Codebook with good accuracy	Requirement of source image for splicing detection
5	Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform [7]	DWT, shift vector	copy-move image forgery	lower computational complexity and detect small size and multiple copy-move forgery	---------------------
6	Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis [8]	DCT, Wavelet decomposition	Spliced Image and Copy-move Forgery	Good accuracy with 81.50%	--------------------
7	Image splicing detection based on inter-scale 2D joint	DWT, PCA, SVM	Splicing forgery detection based on	Attained accuracy 96.2 % for the Columbia	Less accurate with color image and better

	characteristic function moments in wavelet domain [9]		inter-scale 2D joint characteristic function	image splicing detection evaluation dataset.	accuracy with gray image.
8	An Effective Algorithm of Image Splicing Detection [10]	Multi-size Block Discrete Cosine Transform (MBDCT), SVM, Image quality metrics (IQMs)	Spliced Image	acquired highest accuracy rate 89.16%	required 80% training for higher accuracy
9	Effective Image Splicing Detection Based on Image Chroma [11]	Gray level co-occurrence matrix (GLCM), SVM	Gray level co-occurrence matrix used for splicing detection	Shown 96.2% of accuracy over the Columbia Image Dataset	----------------------
10	Pixel Based Digital Image Forgery Detection Techniques [12]	DWT	Copy-move Forgery detection	Robust against rotation	considers only 90°, 180°, 270° angle orientation
11	Fast, automatic and fine-grained tampered JPEG image detection via Discrete Cosine Transform coefficient analysis [19]	DCT	Double quantization effects hidden among histograms of DCT coefficients	Insensitive to the tampering methods	restricted to Image Format

6. PROPOSED WOR

The proposed methodology will deal with image splicing forgery since image splicing is frequently employed method in the domain of image forgery.

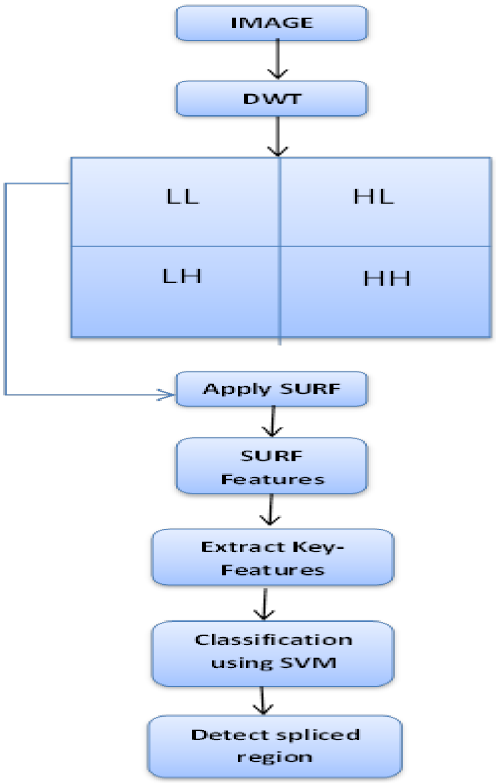


Fig 6: Work Flow of the wavelet-based image splicing forgery detection

To deal with the problem of authenticity as well as integrity, this paper presents an effective blind approach for image splicing detection. Figure 6 shows step by step flow of proposed approach to deal with image splicing forgery, which is initiating with DWT transform and followed by SURF feature extractor and at the end, SVM classifier will used to make decision.

This approach will initiate with image decomposition using DWT transform that will employ on input image to minimize the image size representation. DWT will divide the image into four sub-images which will label as LL, HL, LH and HH. These DWT coefficients are basically approximation image, horizontal detail image, vertical detail image and diagonal detail image respectively. Approximation image *i.e.,* LL part of an image used to contains most of the information of image and detail images *viz;* HL, LH and HH used to contain horizontal, vertical and diagonal edge information of an image. These detail edge information will help to identify the inconsistency between two edge coefficients and approximation image will further decompose by DWT to yield more DWT coefficients. These coefficients will further process with SURF.

After DWT, SURF will apply on the calculated coefficients to extract the specific features of image which will helpful in determining the location as well as orientation and scale parameters of spliced region of an image. As SURF is keypoint-based feature extractor and it shows robustness against scaling and rotation. SURF will extract interest keypoint from decomposed image and generates a descriptor *i.e.,* feature vectors to store the information of extracted features. These feature vectors will contain the information of position of interest point, that further supply to SVM.

At last, Support Vector Machine (SVM) will used to perform classification on the extracted features. On the basis of features produced by SURF, SVM will make decision to classify the image as spliced image or authentic image. And the result will come up with the detection of spliced region if the image is forged.

7. CONCLUSION

All image forgery detection techniques that come under the blind approach have been concisely explained in section 4. In addition, section 4 also analyzed the different types of forgeries in the digital image based on tampering perform with images. This paper presented a brief idea on the types of digital image forgery along with several image forgery detection techniques with respect to tampering that may help research scholars in future to illustrate their ideas to overcome the problem of authentication of the digital image. This survey may provide a new approach to study of digital image forgeries and their detection mechanism with regards to blind approach. This paper also represented a comparison between many image forgery detection techniques along with their advantages and boundaries. This paper concludes that blind approach techniques are effective rather than active approaches as well it provided good accuracy rate.

This paper also tossed an idea on image splicing detection technique using DWT transform to deal with image splicing forgery. The proposed method in the paper is also a blind approached method which did not consider any pre-inserted traces. Rather, it works with the edge information of an image and traces leave as boundary edges inconsistency of tampered region. This method will show robustness over orientation and scaling geometric parameter as SURF is invariant to scaling and rotation.

8. REFERENCES

[1] V. P. Nampoothiri and N. Sugitha, 2016, "Digital Image Forgery - A threaten to Digital Forensics", *IEEE* International Conference on Circuit, Power and Computing Technologies (ICCPCT), 1-6.

[2] C. N. Bharti and P. Tandel, 2016, "A Survey of Image Forgery Detection Techniques", *IEEE* International conference on Wireless Communication, signal Processing and Networking, 877-881.

[3] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, 2013, "Splicing Image Forgery Detection Based on DCT and Local Binary Pattern", *IEEE* Global Conference on Signal and Information Processing, 253-256.

[4] S. D. Lin and T. Wu, 2011, "An Integrated Technique for Splicing and Copy-move Forgery Image Detection", *IEEE* 4th International Congress on Image and Signal Processing, 1086-1090.

[5] Y. Fan, P. Carré and C. Fernandez-Maloigne, 2015, "Image Splicing Detection with Local Illumination Estimation", *IEEE* International Conference on Image Processing (ICIP), 2940-2944.

[6] S. D. Mahalakshmi, K. Vijayalakshmi and E. Agnes, 2013, "A Forensic Method for Detecting Image Forgery", *IEEE* International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 590-594.

[7] P. Yadav, 2012, "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform", *IEEE* International Journal on Computer Science and Engineering (IJCSE), Vol. 4, No. 04, 565-570.

[8] A. Kashyap, R. S. Parmar, B. Suresh, M. Agarwal and H. Gupta, 2017, "Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis", International Conference of Signal Processing and Communication (ICSC), 187-190.

[9] T. H. Park, J. G. Han, Y. H. Moon and K. Eom, 2016, "Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain", *SpringerOpen* EURASIP Journal on Image and Video Processing, 1-10.

[10] Z. Zhang, J. Kang and Y. Ren, 2008, "An Effective Algorithm of Image Splicing Detection", *IEEE* International Conference on Computer Science and Software Engineering, 1035-1039.

[11] W. Wang, J. Dong and T. Tan, 2009, "Effective Image Splicing Detection Based on Image Chroma", *IEEE* International Conference on Image Processing (ICIP), 1257-1260.

[12] P. Deshpande and P. Kanikar, 2012, "Pixel Based Digital Image Forgery Detection Techniques", International Journal of Engineering Research and Applications (IJERA), Vol. 2, No. 3, 539-543.

[13] M. M. Isaaca and M Wilscy, 2015, "Image forgery detection based on Gabor Wavelets and Local Phase Quantization", *ELSEVIER* Second International Symposium on Computer Vision and the Internet (VisionNet'15), 76-83.

[14] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, 2013, "Copy Move Forgery Detection using DWT and SIFT Features", *IEEE* International Conference on Intelligent Systems Design and Applications (ISDA), 189-193.

[15] R. Rajkumar and K. M. Singh, 2015, "Digital Image Forgery Detection using SIFT Features", *IEEE* International Symposium on Advanced Computing and Communication (ISACC), 186-191.

[16] R. M. Rad and K. Wong, 2015, "Digital Image Forgery Detection by Edge Analysis", *IEEE* International Conference on Consumer Electronics-Taiwan (ICCE-TW), 19-20.

[17] K. Khuspe and V. Mane, 2015, "Robust Image Forgery Localization and Recognition in Copy-Move Using Bag of Features and SVM", *IEEE* International Conference on Communication, Information Computing Technology (ICCICT), 1-5.

[18] A. V. Mirea, S. B. Dhokb, N. J. Mistrya and P. D. Poreya, 2015, "Factor Histogram based Forgery Localization in Double Compressed JPEG Images", *ELSEVIER* Eleventh International Multi-Conference on Information Processing (IMCIP), 690-696.

[19] V. Sharma, S. Jha, R. K. Bharti, 2016 , "Image Forgery and it's Detection Technique: A Review", International Research Journal of Engineering and Technology (IRJET), Vol. 3, No. 03, 756-762.

[20] B Shwetha and S V Sathyanarayana, 2017, "Digital image forgery detection techniques: a survey", ACCENTS Transactions on Information Security, Vol. 2(5), 22-31.

[21] Guohui LiI, Qiong WuI, Dan TuI and Shaojie SunI , 2007 , "A Sorted Neighborhood Approach for Detecting

Duplicated Regions in Image Forgeries based on DWT and SVD", *IEEE* International Conference on Multimedia Expo(ICME), 1750-1753.

[22] XiaoBing Kang and ShengMin Wei, 2008, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics", *IEEE* International Conference on Computer Science and Software Engineering, 926-930.

[23] The dataset mentioned in the paper is freely available to reader at the address [online]. Available: http://forensics.idealtest.org/casiav1/

[24] The dataset mentioned in the paper is freely available to reader at the address [online]. Available: http://forensics.idealtest.org/casiav2/

[25] The dataset mentioned in the paper is freely available to reader at the address [online]. Available: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm