An Analysis of Image Forgery Detection Techniques

Article *in* Statistics Optimization & Information Computing · May 2019

DOI: 10.19139/soic.v7i2.542

2 authors, including:

Navdeep Kanwal
Punjabi University
27 PUBLICATIONS **212** CITATIONS

SEE PROFILE

STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **7**, June 2019, pp 486–500.
Published online in International Academic Press (www.IAPress.org)

An Analysis of Image Forgery Detection Techniques

Chandandeep Kaur, Navdeep Kanwal *

Department of Computer Engineering, Punjabi University, India

Abstract Society is becoming increasingly dependent on the internet and so does it become more and more vulnerable to harmful threats. These threats are becoming vigorous and continuously evolving. These threats distorts the authenticity of data transmitted through the internet. As we all completely or partially rely upon this transmitted data, hence, its authenticity needs to be preserved. Images have the potential of conveying much more information as compared to the textual content. We pretty much believe everything that we see. In order to preserve/check the authenticity of images, image forgery detection techniques are expanding its domain. Detection of forgeries in digital images is in great need in order to recover the peoples trust in visual media. This paper is going to discuss different types of image forgery and blind methods for image forgery detection. It provides the comparative tables of various types of techniques to detect image forgery. It also gives an overview of different datasets used in various approaches of forgery detection.

Keywords Image Forgery, Forgery Detection, Fake Pictures, Blind Methods.

DOI: 10.19139/soic.v7i2.542

1. Introduction

Image Forgery is not a modern concept as it comes along with the invention of photography. But it comes in the limelight nowadays, with the invent of easily accessible digital cameras supported with image editing software tools. Image Forgery begins with the first known fake image that was of Hippolyta Bayard, who released a fake picture of him committing suicide as an act of annoyance for the sake of losing the tag of inventor of photography to Louis Daguerre in 1840 [1]. Digital visual media, nowadays, represent one of the prominent technique of exchanging information, because of increase in easy to use and inexpensive devices. Moreover, visual media has greater expressive potential than any of the existing media. It describes convoluted scenes in an uncomplicated manner, whichever in a different way can be quite tough to transcribe. Malicious modification of digital images with intent to deceive for the sake of altering the public perception is termed as Digital Image Forgery. The modification is done in such a way that it hardly leaves any visually detectable traces. Manipulation of Digital images isnt any longer defined to experts with all the arrival and dispersal of handy image editing tools and softwares. Some of the well-known images editing tools available online are Sumopaint, Paintshop Pro, Photoshop CC, HitFilm Express [2]. Manipulation of visual media with such easily available tools is no longer a herculean task [3]. It is not concerned whether an image is fake or not, until or unless it causes some harm. These images are accepted as certification of truthfulness almost by everyone and everywhere. So, confirmation of an images authenticity is needed. Such confirmation is done with the help of image forgery detection techniques. These methods aim at validating the authenticity of images. There are several types of image forgery exposed to date and correspondingly the forgery detection techniques. This paper aims to review the existing types of forgeries and their detection techniques.

*Correspondence to: Navdeep Kanwal (Email: navdeepkanwal@gmail.com). Department of Computer Engineering, Punjabi University, NH64, Patiala, Punjab, India (147002).

ISSN 2310-5070 (online) ISSN 2311-004X (print)

2. Need of Digital Image Forgery Detection

In today s world, it has became so easy to access, process, store and share the information with the availability of handy devices by everyone [2]. Image editing software tools are increasing day by day, leading to the forgery of digital images.The rapid increase in forged images leads to decrease of trust in visual media. Easiness in simulating origin and content of digital visual information, the trustworthiness has always been questioned. It raised the need for forgery detection techniques due to the significant impact of image manipulation on medicine, justice, news reporting and accounting professions [4]. Forgery detection techniques aim to identify inconsistent patterns which are supposed to be present in the image because of manipulation is done in order to forge the image. Active and Passive are the two approaches used for detecting forgery in images. The active approach requires prior information about the image to be embedded into the image itself by using Digital Signature or Digital Watermark in order to detect any manipulation [5], [7]. The passive approach requires no such information about the image to authenticate it. It assumes the fact that although tampering wont leave any visual trace, but they are more likely to modify the image statistics, and these underlying inconsistencies play key role in detection of tampering.

An example of digital image forgery is shown in Figure 1. In this image Malaysian politician Jeffrey Wong Su En was seen being knighted by the Queen of England in July 2010. In Figure 1b the original image was, later on, found out to be of Ross Brown, Formula One Managing Director of Motorsports,accepting the Order of the British Empire from the Queen. Figure 1a later on, found out to be spliced, of Mr. Wongs face and an original ceremony photo, to expand Mr. Wongs fame [6]. Another example of digital image forgery is shown in Figure 2. A leading national party spokesperson shared an image on an Indian news channel which later on found out to be forged as shown in Figure 2. The original image was an iconic image taken by photojournalist Joe Rosenthal in 1945 titled Raising the flag at Iwo Jima taken during World War II as shown in Figure 2. Digital Image Forgery tends to alter the public perception by representing such things which do not even exist. Forgery Detection Techniques aim to verify the authentication of all such information so that it does not mislead the public. Nowadays, every country is adopting the paperless workplaces which lead to storage of data virtually or in digital format, which makes it more vulnerable to get manipulated. It raises the concern of data security. So, researchers took a keen interest in securing

(a) Forged Image (b) Original Image

Figure 1. Example of Digital Image Forgery

(a) Forged Image (b) Original Image

Figure 2. Another example of Digital Image Forgery

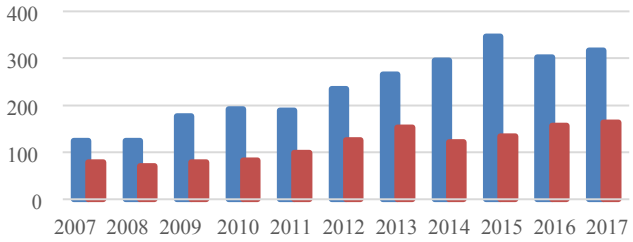


Figure 3. Year wise publications since 2007

the information by developing new forgery detection techniques, over the last decade [1]. For some recent years, research manuscripts in image forensics published by the prominent publishers is shown in Figure 3 [8].

3. Image Forgery Types

The image may be forged either by adding, removing or replacing some regions in the original image with only one thing in mind that it leaves no visually detectable trace. The image can be forged by using several methods, these methods are commonly categorized as in Figure 4:

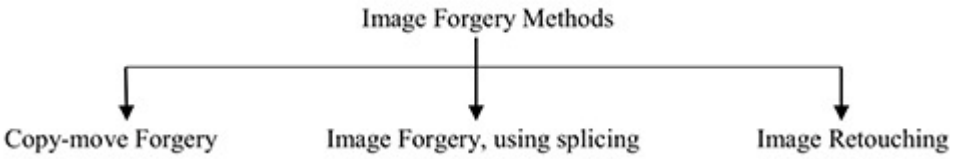
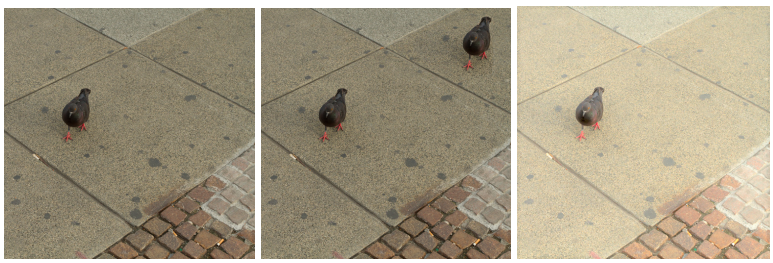


Figure 4. Types of Image Forgery

3.1. Copy Mover Forgery

Copy-Move Forgery involves duplication of part of a picture and then pasted into some other area in the same image as shown in 5b. The intention is to shroud some of the information in the original image. It is the most usually utilized methods to forge an image. As the copied part remains to be of the same image, no visible significant changes are there. Therefore, its detection is usually tough [2] [9].



(a) Original Image (b) Forged Image (c) Image Retouching

Figure 5. Effect of Copy Move Forgery and Image Retouching

(a) First Image (b) Second Image (c) Forged Image

Figure 6. Image Splicing by using two different images

3.2. Image Forgery, using retouching

In this, the image does not fundamentally changes, but there is an enhancement, reduction of a certain feature of the original image as shown in Figure 5c. It is a soft destructive image forgery. It is commonly used by magazine photo editors in order to make photos more attractive. Such enhancement may be ethically wrong.

3.3. Image Forgery, using splicing

It is the composition of one or more images. The images are consolidated to make an altered image. It uses cut/copy and paste operations. A bit of one image is taken and glued into some other image. It needs some post-processing operations in order to completely merge the cut/copied portion of an image into another image as shown in Figure 6. The pasted portion disturbs the pattern of the image. Thus, analysis of image pattern helps in detection of image forgery.

4. Passive Approach of Image Forgery Detection

Image Forgery is commonly done at pixel level because of its simplicity, which leads to the wide utilization of pixel-based methods for detection of image forgery [4]. There are several approaches to pixel level Forgery Detection which are classified as:

4.1. Copy-Move Forgery Detection Techniques

In copy-move forgery, different parts of an image are copied and moved to different locations in the same image. Different parts of an image are strongly correlated in terms of their features. Abrupt features are computed either by dividing an image into overlapping blocks or into disjoint blocks or by computing local key points for the complete image. These features play a key role in copy-move forgery detection [10] [11]. Generalized structure followed by every copy-move forgery detection technique is shown Figure 7 [12]. Operations such as cropping, conversion of an RGB image to grayscale, DCT or DWT transformation are all managed by Preprocessing in order to enhance the classification performance [3]. Feature Extraction and Feature Selection involves the extraction of manipulation sensitive and most informative features out of a set of features of an image. Feature Matching compares the selected features of every block to the other to find any similarity [13] . Forgery is localized by highlighting the similar blocks in an image. Distinctive researchers make utilization of different types of features [14]. These researchers are classified according to the type of feature used in their methods as shown in Figure 8. Some of these methods are discussed as below:

4.1.1. **Transform Domain Based Methods-** In Transform domain, most information about an image is carried by few coefficients. Instead of using all coefficients, we can use these few coefficients in our forgery detection procedure. Copy-Move Forgery Detection in Transform domain is based on:
Frequency: These methods make use of frequency levels of an image. A method was proposed by [2] to detect

image forgery by utilizing Discrete Cosine Transform(DCT) coefficients. The work of [15] also make use of DCT coefficients along with lexicographically sorting. Features are represented by the use of DCT on every single block, then these features are lexicographically sorted to make the method more robust. In this proposed approach, DCT coefficients effectively detect the counterfeited part even when the copied area is improved/modified to totally blend it with background. It may recognizes the forgery even when the counterfeited image is saved using a lossy compression technique, such as JPEG. Considering wavelets as a basis for forgery detection, [16], [17] proposed approaches to detect forgery, by first exerting Discrete Wavelet Transform (DWT) to the input image to produce a diminished dimensional representation. The compacted image is partitioned into intersecting blocks. These blocks are then arranged and copied blocks are recognized utilizing Phase Correlation as comparability criterion. This method takes less time. It provides a higher rate of accuracy. Dyadic wavelet transform (DyWT) based approach was proposed by [18]. It is more suitable than discrete wavelet transform (DWT) due to its shift invariant property. The image is decomposed into subbands. Sets of blocks are orchestrated in light of high likeness utilizing the LL1 subband and high disparity utilizing the HH1 subband. Coordinated sets are recorded as copy-moved. This technique turns out to be robust against rotation and JPEG compression. In another method [19] used Fourier-Mellin Transform (FMT) in order to detect forgery in the image. These features are scale and translation invariant. This method is vigorous to blurring, compression and commotion. But this method consumes a higher amount of time. In order to detect copy-move forgery in the image [20] proposed an approach which uses Polar Harmonic Transform (PHT) and Polar Cosine Transform (PCT). These features are rotation invariant which makes this method computationally efficient.

Dimensionality Reduction: This method tries to reduce dimension feature vectors of an image which helps in speeding up the feature matching process. Forgery is detected by using Principal Component Analysis (PCA) by [21] in order to accelerate the procedure of forgery detection. These features are tough against commotion and lossy compression, it makes the method computationally efficient. In extension to this technique [22] use Kernel-PCA (KPCA) in its approach to give an accurate estimate of the rotation angle and scaling factor in altered blocks whereas [23] use Singular Value Decomposition(SVD) in its approach which is useful in representing 2nd order statistics. Forgery which manipulates higher order statistics is not detectable accurately by this approach.

Spectral Texture: Texture feature is calculated by using transform domain of the image. Gabor features are used by [24] to detect copy-move forgery. This method is tough against JPEG compression. It also provides precise estimation of tampered blocks, rotation angle and scaling factor.

4.1.2. **Spatial Domain Methods-** Spatial domain describes the content of an image by considering the location of pixels in an image. In the spatial domain, pixels are highly correlated which makes computation larger. Forgery detection in the spatial domain is based on: *Key points:* Key points are spatial locations or points in the image that define what is interesting in the image. These are important because of the reason that no matter how image changes, whether it rotates, shrink, expand or distorted, key points remain almost same in the modified image. Keypoint based approaches [25], [26], [27], [28] and [29] makes use of Scale Invariant Feature Transform (SIFT) in their approach, SIFT features are invariant to rotation and scaling. These are vigorous to commotion and changes in brightening conditions. It has increased computational efficiency. But the problem with this approach is that it detects false result also. [30] and [31] have proposed a programmed and strong copy-move forgery identification technique in view of Speed Up Reduced Features (SURF), which distinguishes duplication region with various sizes. It identifies copy-move imitation with a minimum false counterpart for pictures with high resolution. These features are strong to added commotion and obscuring. These are invariant to rotation and scaling. [32] use Mirror

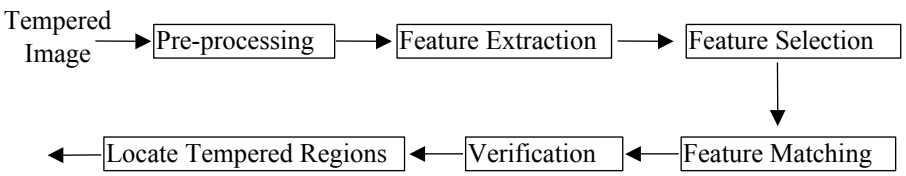


Figure 7. Generalized structure of copy move forgery detection

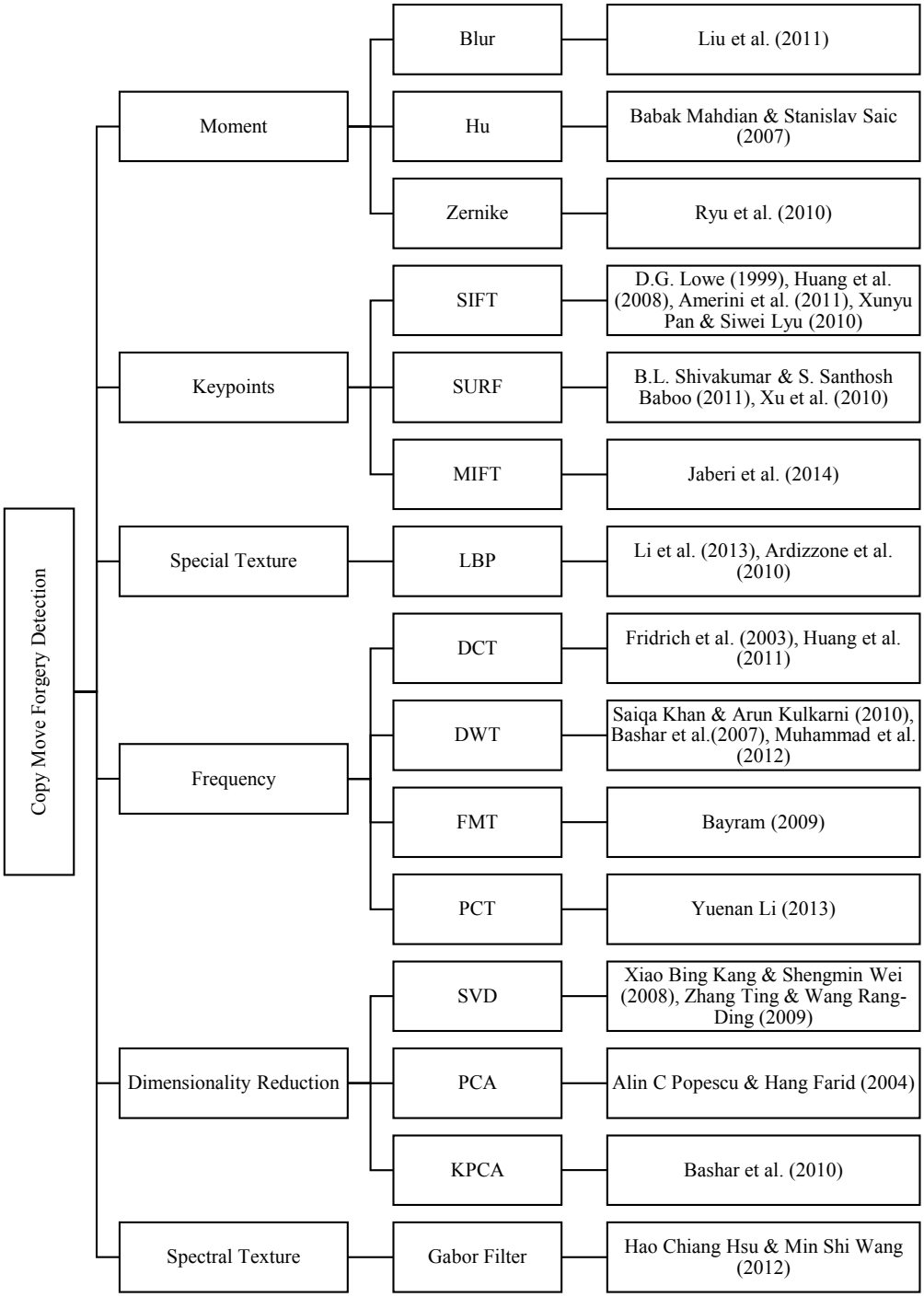


Figure 8. Image Forgery Detection Techniques

Reflection Invariant Feature Transform (MIFT) in its research. MIFT features are helpful in robustly localizing forgery among all available SIFT methods. These are invariant to rotation and scaling. They are invariant to mirror

reflection transformations too. This technique can identify copied areas with higher precision, particularly when the measure of the copied portion is little.

Moments: Moments are a sure specific weighted average of the picture pixels Intensities. The Function of such moments is utilized to get an understanding of a picture in [33]. It make utilization of initial four Hu moments of the circle blocks in order to distinguish and find the copied areas with rotation. While most techniques fall flat when the duplicated region is rotated before being glued, however, this strategy is powerful not exclusively to clamor defilement, obscuring, and JPEG compression yet additionally to the rotation. The proposed technique has better time execution when contrasted with existing strategies on account of the lower feature dimension. [34] proposes a scientific strategy to restrict copied picture regions in view of Zernike moments of small picture blocks. It exploits rotation invariance properties which help in recognizing copied regions regardless of whether the copied area gets pivoted before sticking. It has high strength against JPEG compression, obscuring, added white Gaussian commotion, and moderate scaling. For blur moment invariants [35] proposed a strategy which permits effective identification of copy-move fraud, notwithstanding when copied regions have obscure debasement, extra commotion, or haphazard contrast changes are available in it. This strategy functions admirably for a lossy arrangement, for example, JPEG.

Intensity: Intensity levels of red, green, blue channel of an image are considered in this method [36] which make use of intensity values in its approach. This approach shows that methods in which intensity values are considered as features are robust and can successfully detect copy-move forgery in pictures that have been subjected to different types of post area duplication picture processing like obscuring, clamor sullying, extreme lossy compression, and a blend of these activities. This strategy has bring down computational complexity and is more powerful against stronger attacks.

Spatial Texture: It is the spatial arrangement of color or intensities in an image or a selected region of an image [37]. Image binarization [38] can be used to segmenting foreground of image from background whereas binary pattern classification in local level may help in finding the forgery. [39] utilizes Local Binary Pattern (LBP) as features with a specific end goal to identify imitation. LBP is a sort of gray scale texture operator which is utilized for portraying the spatial structure of the picture texture. This strategy turns out to be vigorous against JPEG compression, rotation, obscuring and commotion sullying.

4.1.3. **Hybrid Methods** Different features have their own pros and cons. Two or more features are combined in order to make a robust technique. Various features are combined by [40], [41] to detect forgery accurately and more precisely and with minimum false positives. Table 1 summarize various techniques of copy move forgery detection techniques.

Table 1. Comparative Table of Copy-Move Forgery Detection Techniques

S.No.	Paper	Publication Year	Method Used	Merits/Demerits
1	Fridrich et al. [2]	2003	DCT	Efficient and reliable Doesnt work for noisy images
2	A.C. Popescu & H. Farid [21]	2004	PCA	It detects forgery even when significant amounts of corrupting noise are present
3	W. Luo & J. Huang [36]	2006	Intensity levels	Have lower computational complexity
4	B. Mahdian & S. Saic [35]	2007	Blur Moment Invariant	Robustness for post processing operations Works well for both lossy and lossless formats

5	Li et al. [40]	2007	DWT + SVD	Robust against blurring, added noise and change in contrast. Low computational complexity Accurately localize the highly compressed or edge processed duplicated regions
6	Bashar et al. [17]	2007	DWT	Efficient and robust approach
7	Hailing et al. [26]	2008	SIFT	Robust against compound image processing Not robust against small tampered region
8	Bayram [19]	2009	FMT	Time efficient Robust against lossy compression, scaling and rotation
9	Z. Ting & W. Rang-Ding [23]	2009	SVD	Lower computational complexity Does not work well for lossy compression
10	X. Pan & S. Lyu [29]	2010	SIFT	Robust against noise
11	Pan et al. [28]	2010	SIFT	Good detection rate for refined forgeries Smaller replicated regions are difficult to detect
12	Xu et al. [31]	2010	SURF	Fast method Robust against additive noise, blurring and rotation
13	S. Khan & A. Kulkarni [16]	2010	DWT	High accuracy Require less time
14	Bashar et al. [22]	2010	KPCA+DWT	Reduces false detection Works well in noisy and compressed image Cannot handle scaling and shearing geometric operation
15	Amerini et al. [27]	2011	SIFT	Precisely localize tampered area Detect multiple cloning Reliable
16	B. L. Shivakumar & S. S. Baboo [30]	2011	SURF + KD-Tree	Have minimum false matches for high resolution images Cannot detect small copied regions
17	Liu et al. [33]	2011	Hu moments	Performance efficient It discards the Hu moments outside the inscribed circle which affect false forgery detection
18	Huang et al. [15]	2011	DCT	Lesser number of features to represent a block causing better effectiveness Robust against JPEG compression, blurring, AWGN distortion
19	Ghorbani et al. [41]	2011	DWT + DCT(QCD)	Does not detect forgery accurately for rotated or scaled copied region
20	Muhammad et al. [18]	2012	DyWT	Perform well in fixed or variable size images, to detect forgery with or without rotation
21	H.C. Hsu & M.S. Wang [24]	2012	Gabor descriptor	Reliable and robust Have higher accuracy rate, estimated rotation angle and scaling factor
22	Ryu et al. [34]	2013	Zernike Moments	Robust against blurring, additive white Gaussian noise, JPEG compression, and moderate scaling can not localize tampered regions that underwent affine transformations except rotation.
23	Li et al. [39]	2013	LBP + PHT	Robust against region rotation, flipping, blurring, JPEG compression Cannot detect forgery when a duplicated region is rotated at general angles.
24	Y. Li [20]	2013	PCT	High accuracy

25	Jaberi et al. [32]	2014	MIFT	The accuracy rate is high Detect forgery in the small size tampered region Does not work well for flat surface duplicated regions
26	Thampi et al. [42]	2016	Segmentation	The proposed method can withstand postprocessing operations like blurring, noise addition and also geometric transformations such as rotation, scaling, JPEG compression etc.
27	Fan Yang et al. [43]	2017	KAZE + SIFT	It can precisely detect the tampered regions, even if the pasted region has undergone several transformations such as rotation, scaling, JPEG compression.
28	Bhanu et al. [44]	2017	Segmentation + SURF + Knn (K-nearest neighbor)	This method reduces forgery detection time. It gives reduced false positive rate.
29	Emam et al. [45]	2017	Difference of Gaussians (DOG) operator + Multi-supportt region order-based gradient histogram (MROGH) descriptor	This method is robust when compared with the state-of-the-art methods. It can detect forgery even from smooth regions.
30	Chou et al. [46]	2018	Local Gabor wavelets patterns (LGWP) + Gabor + Filter+Local binary pattern (LBP)	It can precisely locate the tampered regions, even if the forged image is distorted by JPEG compression, blurring, rotation etc.

4.2. Image Splicing Detection Techniques

Image Splicing Detection Methods aims at finding splicing sensitive features and any disturbance in image patterns which are present in the image because of cut and pasted regions. Every detection method follows a generalized structure as shown in Figure 9. In this generalized structure, Preprocessing manages activities, for example, editing, changing the RGB picture into grayscale, DCT or DWT change to enhance the categorization performance [3]. Feature Extraction and Feature Selection involves the extraction of most informative features out of a set of features of an image. Classifier in this model are trained to distinguish whether a picture is legitimate or interfered, with the assistance of extracted features of various images of different datasets available. [47] examines the image run-length portrayal and sharp image attributes as a discontinuity in image pixel correlation and coherency which is triggered by splicing. Image Run length portrayal and image edge statistics like features are utilized to recognize splicing in it. Another paper [48] calculates the approximate run length along edge gradient direction utilizing computed edge gradient matrix. A few features are extracted from surmised Run length histogram. To get more features, Approximate run length is applied to anticipate error images and this remade image in view of DWT is utilized as a part of image splicing detection. Further, [49] expanded this idea by the original Markov features given by [50], to capture intra-block as well as the inter-block correlation between BDCT coefficients. More features are extricated in DWT space to describe positions, scales, orientations dependency among wavelet coefficients. Then, SVM-RFE is utilized to lessen the features. After then, SVM distinguishes the original and spliced image. [51] proposes a strategy where Markov features in spatial and Discrete Cosine Transform Domains are extricated and consolidated to detect forgery. Principal Component Analysis (PCA) chooses the most pertinent features. With the assistance of the radial basis function kernel, an enhanced SVM is built to distinguish forged and legitimate images. This method

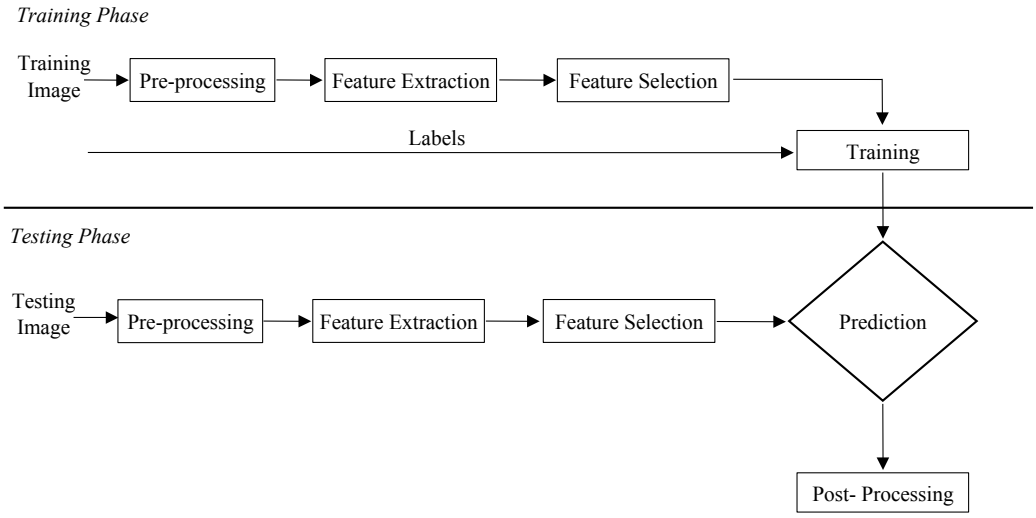


Figure 9. Generalized model of image splicing forgery detection

provides higher accuracy with the minimum use of feature dimension. Local Binary Pattern (LBP) based approach is proposed in [52], which firstly divides the chrominance component of the input image into intersecting blocks. LBP is calculated for each block and afterward each blocks LBP is changed into frequency domain utilizing 2D DCT. Standard deviations of separate frequency coefficient of each block are computed and utilized as features. [53] handles high dimensionality and repetition in extricated features effectively. It proposes a strategy to enhance Run Length Run Number (RLRN) algorithm by applying PCA and KPCA dimension diminishment technique to decrease computational time. Afterwards, SVM characterizes the bonafide and altered pictures.

DCT coefficients are used by [27] as first digit features to distinguish and confine a solitary and a twofold JPEG compression in small segments of a picture. It defeats the constraint of proving multi-JPEG compression in a full-frame picture. SVM is utilized to classify the picture in this technique. Another splicing approach [54] recognizes image splicing based on an irregularity in the obscure degree and profundity data of a picture. Subsequent to evaluating the local obscure kernels of picture blocks, the multistep re-obscuring procedure is utilized to quantify relative obscure degrees of assessed local obscure kernels. These relative obscure degrees are utilized to classify the picture block. Any irregularity in obscure degree is utilized as a confirmation of picture splicing. [55] proposes a method which extracts two groups of features from first-order histogram of DWT coefficients of the image and Hilbert Huang Transform (HHT) of the image. These extracted features are fed to SVM to help it in classifying real and spliced image. A comparison of different methods of image splicing is presented in Table 2

4.3. Image Retouching Detection Techniques

Image Retouching Detection methods aim to detect inpainting forgery. It is a forgery type where copied information is non-continuous.

[56] rated the photographs on a metric (1-5) by estimating geometric and photometric changes done to an image with the help of digital photo-editing techniques. Minimum metric value represents the least retouching done to an image and maximum value represent a huge amount of retouching. Geometric changes were calculated with 4 measurements: mean and standard deviation of motion magnitude which is figured independently for body and face of the object and Photometric changes were estimated using 4 measurements: mean and standard deviation of spatial limits of sharpening/smoothing filters and Structural Similarity Index Metric (SSIM). A three step method is proposed in [57] where inpainting detection is done. It makes use of patches and three global parameter thresholds. In the first step, it looks out for all pairs of similar patches using similarity measure, distance measure and cardinality measure. In the second step, tampering mask is generated with localization of matched patches. In order to reduce false detected patches, it makes use of filtering scheme in the third step. The human judgment of

Table 2. Comparative Table of Image Splicing Forgery Detection Techniques

S. No.	Paper Title	Publication Year	Features Extracted	Classifier Used	Dataset Used	Feature Dimension	Accuracy Rate as claimed (%)
1	Dong et al. [47]	2009	Run length and Image edge statistics	SVM	CISDE	61	76.52
2	Zhang et al. [23]	2009	Markov & CCPM of DCT	SVM	CISDE	109	91.5
3	Li et al. [55]	2010	HHT & DWT coefficient histograms	SVM	CISDE	72	85.87
4	He et al. [48]	2011	Approximate Run Length(ARL)	SVM	CISDE	30	80.58
5	He et al. [49]	2012	BDCT Markov & DWT Markov	SVM + RFE	CISDE CASIA v2.0	100 Y-100	93.55 89.76
6	A. A. Alahmadi et. al [52]	2013	LBP & DCT	SVM	CASIA v1.0 CASIA v2.0	- -	97 97.5
7	Moghaddasi [53]	2014	RLRN & PCA/KPCA	SVM	CISDE CASIA v1.0	50 Y-50 Cb-50 Cr-50	88.28 88.28 89.36 88.31
8	El-Alfy et. al [51]	2015	BDCT Markov & Spatial	SVM + PCA	CISDE	50	98.22

beauty utilizing different features like localization of face, eye, pupil, eyebrows, thebase of the nose, lip, chin is measured in [58]. Several impermanent features like make-up, haircut, presence of glasses likewise influence the human judgment of beauty is proved by [59]. A novel dataset SCUT-FBP [65] is proposed which contains pictures of 500 Asian female alongside appeal appraisals, for facial beauty perception. This rating is performed with various blends of facial geometrical features and texture features utilizing machine learning and deep learning techniques.

An efficient forgery detection algorithm [60], which integrated central pixel Mapping (CPM) a speed-up method for finding suspicious blocks with similar hash-values, greatest zero connectivity component labeling (GZCL) marks the tampered pixels in suspected block pairs and fragment splicing detection (FSD)which denotes the altered pixels in presumed block pairs and fragment splicing detection (FSD) which recognizes and locates the altered regions from its best match areas to detect image altering. Chang et al. [61] proposed a strategy which distinguishes the forged regions, even for images having a uniform background. This technique contains two procedures. A suspicious area location process which looks through the similitude blocks to discover suspicious regions, it utilizes comparability vector to decrease false positives. Forged region identification process which makes utilization of multi-region realtion (MRR) to distinguish tampered areas.

Table 3. Description of the various MICC copy-move forgery datasets

Dataset	Total No. of images	No. of authentic images	No. of tampered images	Image type	Image format	Image resolution
MICC-F2000[27]	2000	1300	700	Color	JPEG	2048*1536
MICC-F220 [27]	220	110	110	Color	JPEG	722*480, 800*600
MICC-F600 [27]	600	440	160	Color	PNG	3264*2448

5. Datasets available for Image Forgery Detection

To evaluate the performance and validate the results of different forgery detection methods, benchmarked image forgery datasets are required. There are a few freely accessible datasets for copy-move forgery, image splicing forgery and image retouching forgery available. A concise description of accessible datasets is given beneath:

5.1. Copy-move forgery datasets

MICC-F2000, MICC-F220, MICC-F600 AND CoMoFoD are available data sets to evaluate the performance of copy-move forgery detection algorithm. The altered pictures in these datasets are made by replicating small patches of the image and moving these patches onto some other location in the same image. Diverse post-processing activities (e.g., Rotation, Scaling, Translation or their blend) have been performed on these small patches in order to merge them completely in the image. The underlying facts behind the copy-move forgery is not provided in MICC-F2000 but is provided in MICC-F600 dataset. A detailed illustration of the copy-move forgery datasets is abridged in Table3.

CoMoFoD [62] dataset has 260 image sets, which is divided into small image category and large image category. Images are grouped in 5 groups. Every image set comprises of original images, colored mask, binary mask and forged image.

- Small Image Category Database:
  - It has 200 image sets
  - Images of resolution 512*512
  - Contains 40 images per transformation type
  - Total number of images with postprocessed images are 10400
- Vast Image Category Database:
  - It has 60 image sets
  - Images of resolution 3000*2000
  - Consists 10/20 images per transformation type
  - Total number of images with postprocessed images are 3120

5.2. Image Splicing Datasets

Digital Video and Multimedia Lab (DVMM), at Columbia University created the first image splicing dataset which is Columbia Image Splicing Detection Evaluation(CISDE) dataset [63]. CISDE dataset is for gray images. For color images, DVMM developed Columbia Uncompressed Image Splicing Detection, Evaluation (CUISDE) dataset [64].

Another image grafting dataset is given by the Chinese Academy of Sciences, Institute of Automation (CASIA). It gives the CASIA Tampered Image Detection Evaluation (TIDE) v1. 0 dataset and CASIA TIDE v2.0. CASIA

Table 4. Description of Image Splicing Datasets

Dataset	Total no. of Images	No. of authentic Images	No. of tampered Images	Image type	Image format	Image resolution
CISDE [63]	1845	933	912	Gray	BMP	128*128
CUISDE [64]	363	183	180	Color	TIFF	757*568, 1152*768
CASIA v1.0 [65]	1721	800	921	Color	JPEG	384*256
CASIA v2.0 [66]	12,614	7491	5123	Color	JPEG BMP TIFF	240*160 to 900*600

v2.0 is a broadened variant of CASIA v1.0 dataset [65, 66]. Altered images in these datasets are made utilizing splicing operation from at least two images. With a specific end goal to leave no visually detectable trace, different post-processing activities and geometric changes such as rotation, scaling and obscuring is applied on the tampered images. A detailed illustration of image splicing datasets is given in Table 4.

6. Conclusion and Future Scope

The quickly developing enthusiasm for discovering passive techniques to approve the validness of a picture has been seen throughout the most recent decade, in light of the significance advanced visual media plays in our life. This paper introduced an overview of various passive image forgery detection techniques. A comparative analysis of various forgery detection techniques is also presented. This paper also provides various types of data sets utilized in the different approaches of forgery detection. The foremost drawback of the existing detection techniques which can be worked on, is that the detection of forgery in proposed techniques needed human intervention. Another major drawback in the discussed methods until now is that they do not succeed in differentiating malicious tampering from innocent retouching. Also, the discussed methods specifically detect the forgery type for which they are developed, they cannot detect any other forgery type present in the image. So, a unified robust method to identify any type of forgery in the image is needed. There is a scope for extending the passive-blind forgery detection for audio and video tampering. With the development of sophisticated artificial intelligence techniques, a promising solution for digital image forensics is suggested. Although deep-learning-based approaches are promising, but they are not powerful enough to give good performance in several digital image forensics applications. A considerable amount of work is needed to be done on all these parameters.

REFERENCES

1. M. Ali and M. Deriche, *A bibliography of pixel-based blind image forgery detection techniques*, Signal Processing Image Communication, vol. 39, pp. 46–74, 2015.
2. J. Fridrich, D. Soukal and J. Lukáš, *Detection of Copy-Move Forgery in Digital Images*, International Journal, vol. 3, pp. 652–663, 2003.
3. K. G. Birajdar and V. H. Mankar, *Digital image forgery detection using passive techniques: A survey*, Digital Investigation, vol. 10, pp. 226–245, 2004.
4. A. Kashyap, R. S. Parmar, M. Agrawal and H. Gupta, *An Evaluation of Digital Image Forgery Detection Approaches*, ISSN 09739769, 2017.
5. K. Sreenivas and Kamkshi Prasad, V., *Fragile watermarking schemes for image authentication: a survey*, International Journal of Machine Learning and Cybernetics, 2017.
6. *Photo Tampering throughout History*, izitru, Available: http://pth.izitru.com/, [Accessed: 29-May-2018].
7. N. Kaur and N. Kanwal, *Review And Analysis of Image Forgery Detection Technique for Digital Images*, International Journal of Advanced Research in Computer Science, vol. 8, pp. 172–175, 2017.

8. N. Kanwal, J. Bhullar, L. Kaur, and A. Girdhar, *A Taxonomoy and Analysis of Digital Image Forgery Detection Techniques*, Journal of Engineering, Science & Management Education, vol. 10, pp. 35–41, 2017.
9. Z. Zhang , C. Wang, X. Zhou, *A survey on passive image copy-move forgery detection*, Journal of Information Processing Systems, vol. 14, no. 1, pp. 6–31, 2018.
10. D. Chauhan, D. Kasat, S. Jain and V. Thakare, *Survey on Keypoint Based Copy-move Forgery Detection Methods on Image*, Procedia Computer Science, vol. 85, pp. 206–212, 2016.
11. O.M. Al. Qershi and B. E. Khoo, *Passive detection of copy-move forgery in digital images: State-of-the-art*, Forensic Science International, vol. 231, pp. 284–295, 2013.
12. N. K. Gill, R. Garg, and A. Doegar, *A review paper on digital image forgery detection techniques*, Proc. IEEE 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7, 2017.
13. O.M. Al. Qershi and B. E. Khoo, *Comparison of Matching Methods for Copy-Move Image Forgery Detection*, Proc. Springer 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, pp. 209–218, 2017.
14. B. Soni, P. K. Das and D. M. Thounaojam *CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection*, IET Image Processing, vol. 12, pp. 167–178, 2017.
15. Y. Huang, W. Lu, W. Sun, and D. Long, *Improved DCT-based detection of copy-move forgery in images*, Forensic science international, vol. 206, pp. 178–184, 2011.
16. S. Khan and A. Kulkarni, *An efficient method for detection of copy-move forgery using discrete wavelet transform*, International Journal on Computer Science and Engineering, vol. 2, pp. 1801-1806, 2010.
17. Md. K. Bashar, K. Noda, N. Ohnishi, H. Kudo, T. Matsumoto and Y. Takeuchi, *Wavelet-Based Multiresolution Features for Detecting Duplications in Images* Proc. Mach. Vis. Appl., pp. 264-267, 2007.
18. G. Muhammad, M. Hussain, and G. Bebis, *Passive copy move image forgery detection using undecimated dyadic wavelet transform*, Digital Investigation, 9, pp. 49-57, 2012.
19. S. Bayram, H. T. Sencar, and N. Memon, *An efficient and robust method for detecting copy-move forgery*, Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2009, pp. 1053–1056, 2009.
20. Y. Li, *Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching*, Forensic science international, vol. 224, pp. 59–67, 2013.
21. A.C. Popescu, and H. Farid, *Exposing digital forgeries by detecting duplicated image regions*, Technology Report TR2004-515 by Department Computer Science, Dartmouth College, 2004.
22. M. Bashar, K. Noda, N. Ohnishi, and K. Mori, *Exploring duplicated regions in natural images*, IEEE Transactions on Image Processing, 2010.
23. T. Zhang and R.D. Wang, *Copy-move forgery detection based on SVD in digital image*, Image and Signal Processing, IEEE-CISP'09. 2nd International Congress on, pp. 1–5, 2009.
24. H. C. Hsu and M. S. Wang, *Detection of copy-move forgery image using Gabor descriptor*, Anti-counterfeiting, security and identification (ASID), 2012 IEEE international conference on, pp. 1–4, 2012.
25. D. G. Lowe *Object recognition from local scale-invariant features*, Computer vision, 1999. The proceedings of the seventh IEEE international conference on, vol. 2, pp. 1150–1157, 1999.
26. H. Huang, W. Guo, and Y. Zhang, *Detection of copy-move forgery in digital images using SIFT algorithm*, Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, vol. 2, pp. 272–276, 2008.
27. I. Amerini, L. Ballan, R. Caldelli, B. A. Del and G. Serra, *A sift-based forensic method for copy–move attack detection and transformation recovery*, IEEE Transactions on Information Forensics and Security, vol. 6, pp. 1099–1110, 2011.
28. X. Pan and S. Lyu, *Detecting image region duplication using SIFT features*, Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, pp. 1706–1709, 2010.
29. X. Pan, and S. Lyu, *Region duplication detection using image feature matching*, IEEE Transactions on Information Forensics and Security, vol. 5, pp. 857–867, 2010.
30. B. L. Shivakumar, and S. S. Baboo, *Detection of region duplication forgery in digital images using SURF*, International Journal of Computer Science Issues (IJCSI), vol. 8, no. 4, pp. 199, 2011.
31. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, *Image copy-move forgery detection based on SURF*, Multimedia information networking and security (MINES), International conference on, pp. 889–892, 2010.
32. M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, *Accurate and robust localization of duplicated region in copy-move image forgery*, Machine vision and applications, vol. 25, pp. 451–475, 2014.
33. G. Liu, J. Wang, S. Lian, Shiguo and Z. Wang, *A passive image authentication scheme for detecting region-duplication forgery with rotation*, Journal of Network and Computer Applications, vol. 34, pp. 1557–1565, 2011.
34. S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, *Rotation invariant localization of duplicated image regions based on Zernike moments*, IEEE Transactions on Information Forensics and Security, vol. 8, pp. 1355–1370, 2013.
35. B. Mahdian, and S. Saic, *Detection of copy–move forgery using a method based on blur moment invariants*, Forensic science international, vol. 171, pp. 180–189, 2007.
36. W. Luo, J. Huang and G. Qiu, *Robust detection of region-duplication forgery in digital image*, Proceedings of the IEEE Computer Society, 18th International Conference on Pattern Recognition, vol. 4, pp. 746–749, 2006.
37. E. Ardizzone, A. Bruno and G. Mazzola, *Copy-move forgery detection via texture description*, Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, pp. 59–64, 2010.
38. W. A. Khawand, S. Kadry, R. Bozzo and K. Samaili, *Accurate, Swift and Noiseless Image Binarization*, Statistics, Optimization and Information Computing, vol. 4, pp. 42–56, 2016.
39. L. Li, S. Li, H. Zhu, S-C. Chu, J. F. Roddick and J. S. Pan, *An efficient scheme for detecting copy-move forged images by local binary patterns*, Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46–56, 2013.
40. G. Li, Q. Wu, D. Tu, and S. Sun, *A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD*, Multimedia and Expo, 2007 IEEE International Conference on, pp. 1750–1753, 2007.

41. M. Ghorbani, M. Firouzmand, and A. Faraahi, *DWT-DCT (QCD) based copy-move image forgery detection*, Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on, pp. 1–4, 2011.
42. S. M. Thampi, A. Gelbukh and J. Mukhopadhyay, *Advances in signal processing and intelligent recognition systems*, Proceedings of Second International Symposium on Signal Processing and Intelligent Recognition Systems (SIRS-2015), vol. 425, pp. 645–654, 2016.
43. F. Yang, J. Li, W. Lu and J. Weng, *Copy-move forgery detection based on hybrid features*, Engineering Applications of Artificial Intelligence, vol. 59, pp. 73–83, 2017.
44. M. P. B., Bhavya and A. Kumar, *Copy-move forgery detection using segmentation*, Intelligent Systems and Control (ISCO), 2017 11th International Conference on, pp. 224–228, 2017.
45. Emam, Mahmoud and Han, Qi and Li, Qiong and Zhang, Hongli, *A robust detection algorithm for image Copy-Move forgery in smooth regions*, Circuits, System and Simulation (ICCSS), 2017 International Conference on, pp. 119–123, 2017.
46. Chou, Chao-Lung and Lee, Jen-Chun, *Copy-Move Forgery Detection Based on Local Gabor Wavelets Patterns*, International Conference on Security with Intelligent Computing and Big-data Services, pp. 47–56, 2017.
47. J. W. Dong, T. Wei, S. Tieniu and Q. Yun, *Run-length and edge statistics based approach for image splicing detection*, Springer International workshop on digital watermarking, pp. 76–87, 2008.
48. Z. He, W. Sun, W. Lu and H. Lu, *Digital image splicing detection based on approximate run length*, Pattern Recognition Letters, vol. 32, pp. 1591–1597, 2011.
49. Z. He, W. Lu, W. Sun and J. Huang, *Digital image splicing detection based on Markov features in DCT and DWT domain*, Pattern Recognition, vol. 45, pp. 4292–4299, 2012.
50. Y. Q. Shi, C. Chen and W. Chen, *A natural image model approach to splicing detection*, Proceedings of the 9th ACM workshop on Multimedia & security, pp. 51–62, 2007.
51. El-Alfy, M. E. -Sayed and M. A. Qureshi, *Combining spatial and DCT based Markov features for enhanced blind detection of image splicing*, Pattern Analysis and Applications, vol. 18, pp. 713–723, 2015.
52. A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad and G. Bebis, *Splicing image forgery detection based on DCT and Local Binary Pattern*, Proc. of IEEE Global Conference on Signal and Information Processing (GlobalSIP), pp. 253–256, 2013.
53. Z. Moghaddasi, H. A. Jalab, N. R. Md and S. Aghabozorgi, *Improving RLRN image splicing detection with the use of PCA and kernel PCA*, The Scientific World Journal, vol. 2014, pp. 1–10, 2014.
54. K. Bahrami, A. C. Kot and J. Fan, *Splicing detection in out-of-focus blurred images*, Information Forensics and Security (WIFS), 2013 IEEE International Workshop on, pp. 144–149, 2013.
55. X. Li, T. Jing and X. Li, *Image splicing detection based on moment features and Hilbert-Huang Transform*, Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on, pp. 1127–1130, 2010.
56. E. Kee and H. Farid, *A perceptual metric for photo retouching*, proceedings of the national academy of sciences, vol. 108, pp. 19907–19912, 2011.
57. D. T. Trung, A. Beghdadi and M. G. Larabi, *Blind inpainting forgery detection*, Proc. of Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on, pp. 1019–1023, 2014.
58. H. Gunes and M. Piccardi, *Assessing facial beauty through proportion analysis by image processing and supervised learning*, International journal of human-computer studies, vol. 64, no. 12, pp. 1184–1199, 2006.
59. A. Dantcheva and J. L. Dugelay, *Female facial aesthetics based on soft biometrics and photo-quality*, Proc. of ICME, 2011.
60. D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, Leida and X. Sun, *A robust forgery detection algorithm for object removal by exemplar-based image inpainting*, Multimedia Tools and Applications, vol. 77, no. 10, pp. 11823–11842, 2018.
61. Y. F. Hsu and S. F. Chang, *Detecting image splicing using geometry invariants and camera characteristics consistency*, Multimedia and Expo, IEEE International Conference on, pp. 549–552, 2006.
62. D. Tralic, I. Zupancic, S. Grgic, M. Grgic, *CoMoFoD - New Database for Copy-Move Forgery Detection*, in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, 2013.
63. T.-T. Ng and S. Chang, *A Data Set of Authentic and Spliced Image Blocks*, Columbia University Technical Report, 2004.
64. J. Hsu and S.-F. Chang, *Columbia Uncompressed Image Splicing Detection Evaluation Dataset*, Available: http://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/, [Accessed: 10-May-2018].
65. W. Wang and J. Dong, *CASIA v1.0, Tampered Image Evaluation Database*, Available: http://forensics.idealtest.org/casiav1/, [Accessed: 29-May-2018]
66. W. Wang and J. Dong, *CASIA v2.0, Tampered Image Evaluation Database*, Available: http://forensics.idealtest.org/casiav2/, [Accessed: 29-May-2018]