CHAPTER 2

REVIEW OF LITERATURE

In recent years, the need for the forgery detection algorithm is increasing because of the rapid growth and availability of the imaging processing softwares and the advancements made in digital cameras Snigdha K et al., (2015). Moreover, the necessity ascends because of the bearing of image originality in different environment such as forensic investigation, criminal investigation, law enforcement, journalist photography etc. A minute mislead in the authenticity have greater effect. Moreover in the present information era, the massive images are available in the internet. For any malicious purpose, the image from the web can be collected and altered for the planned purpose. In every aspect of society, the forged image is found to be blow-out for misleading or illegal purposes. It is precisely necessary to analyse these images to establish their authenticity. Either the tampering is done with mislead intention or not, authenticity is obligatory. Bearing in mind the wide range of fields where the influence of tampered image seems intolerable, the need for the reliable, efficient technique for image forgery detection is increasing Farid H (2006), Pearson H (2005), A. C. Popescu and H. Farid(2004). Many of the state of art image forgery detection techniques have been proposed in recent years.

Image forgery detection technique aims to authenticate the originality of the image and localize the tampered region in the image. This area of research is relatively new and only few contributions have been made that relate to the detection of the image forgeries. Forgery detection is the view point of this research. For any investigation to be held it is important to know about the existing concepts and methodologies in the corresponding filed. Only through thorough analysis, the fact for incorporating new concepts can be made. In such cases, the literature is the viable solution.

Literature presents variety of the forgery detection techniques for the originality validation of the image. A detailed survey has been carried out to identify the various research articles available in the literature in all the categories of the forgery detection techniques. The major contributions made in the existing works are analysed with specific mention to the advantages and disadvantages in the literature. In the following sections, the relevant literature applicable for the valuation of the state-of-art work on the image forgery detection technique is provided.

2.1 Categorization of Image forgery Detection techniques

The categorization of the existing research works related to the image forgery detection is deliberated in this section. The image forgery detection techniques are majorly categorized into two types M. Sridevi (2012); i) Active approaches and ii) Passive approach. In the active approaches of the forgery detection, two categories are present. They are

i) Watermark based techniques
ii) Signature based techniques

But in the passive approaches, the category realization is ambiguous. The uncertainty is because of the different types of the forgery practiced over the images. For every tampering action, a suitable detection approaches is obligatory. In current malicious trend, new types of forgeries come into existence every day, for the mere action, new detection techniques are being developed which makes the categorization knotty. Based on the survey conducted, in the passive approaches, seven different categories of detection techniques are discussed. They are

i) Copy-move detection techniques
ii) Splicing detection techniques
iii) Camera based detection techniques

iv) Image enhancement based detection techniques

v) Image format based detection techniques

vi) Shadow based detection techniques and

vii) Reflection based detection techniques

Based on the detailed survey conducted over the image forgery detection techniques, taxonomy is developed for realising the different approaches. The taxonomy provided in this research is not universally acceptable one. However, it aids in differentiating the various active and passive approaches of the image forgery detection technique. Figure 2.1 depicts the literature taxonomy of the image forgery detection techniques.

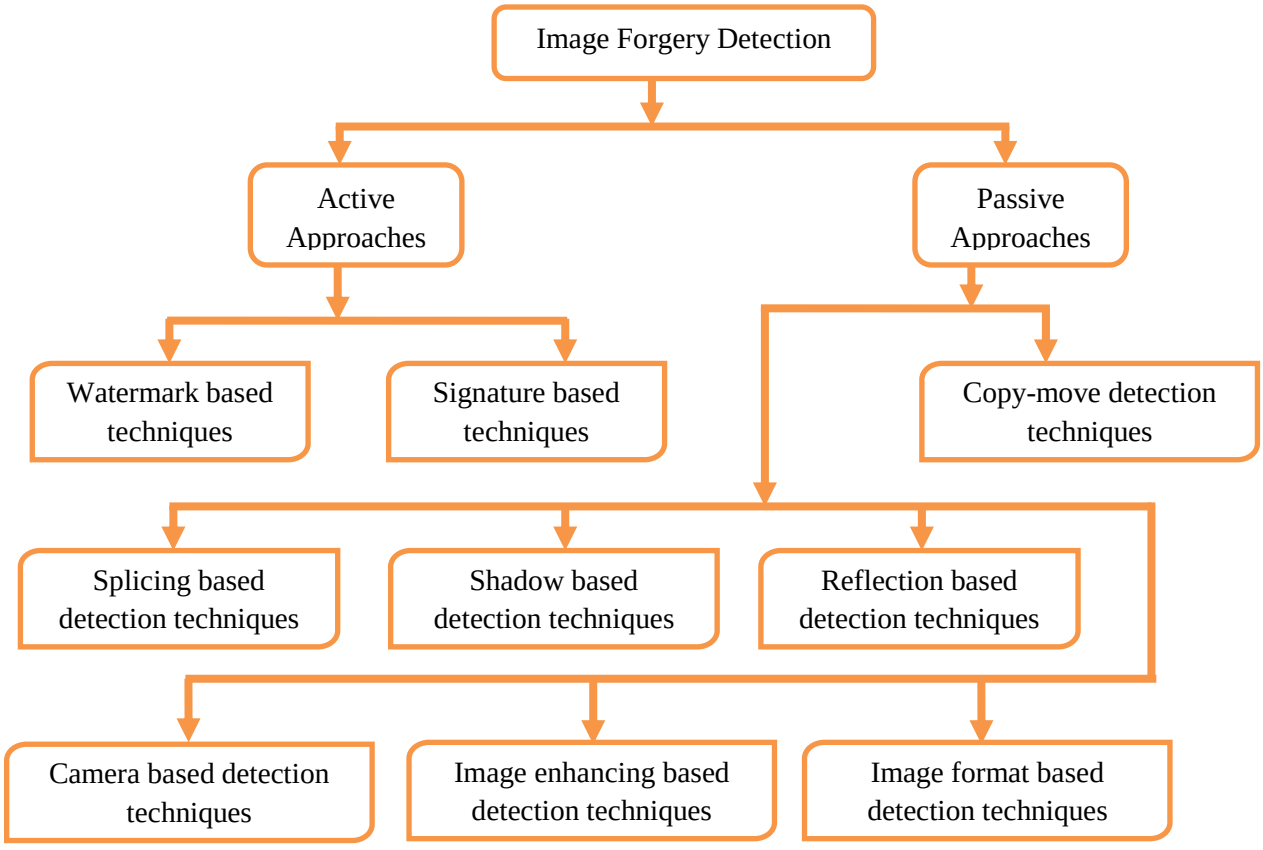

Figure 2.1 Literature taxonomy

2.2 Review of Active approaches based forgery detection

Active approaches are the traditional image forgery detection techniques. In active forgery detection procedure, some entities are embedded into the image before the release of the image. The insertion must be done in a way which is invisible to the human eye i.e. below the human perception level. At the receiving end, the image entity inserted is extracted and verified for authenticity check. The verification of the hidden entity authenticates the originality of the image. The entity embedded into the image is digital watermark or digital signature based on which the active approaches based forgery detection technique is classified into (i) Water mark based detection techniques and Digital Signature based detection technique. Coarsely, the active approaches are classified into unique types based on the method adopted for embedding the entities such as quantization based, feature point based, relation based P. Moulin, R.Koetter (2005), Kutter et al (1999), Hsu et al (1999) etc. The description of the existing research works related to the active image forgery detection approaches is discussed below,

2.2.1 Water mark based detection techniques

In watermark based detection techniques Kundur, D. and Hatzinakos, D(1999), Xiang Zhou et al (2004), the digital watermarks are embedded into the original image at time of capture or in processing stages. The watermark must be engaged in a way with the ability to sustain the removing attack of the unintentional distortion. The originality of the image is verified by comparing the watermark extracted from the image and the original watermark inserted into the image. The change in the watermark corresponds to the modification made in the image which deliberates the tampering action.

DeepaKundur et al(1999) proposed an active approaches for image forgery detection technique. In this method, the watermarking approaches was performed

by embedding a watermark into the discrete wavelet domain of the image unlike traditional approaches, where the watermark is placed in the spatial domain of the signal. This method is a type of quantization based active approaches. The watermark is embedded by quantizing the corresponding coefficients of the image to a pre-specified degree. This method was found to be effective in detecting the versatility. Moreover, their method also helped in characterising the signal modification from some distortion such as filter, lossy compression etc. The watermark insertion using the quantizing coefficient offered the flexibility to make this approaches sensitive to changes in the signal as desired. Capability to ensure the credibility of the image was also found optimal in this method. In the authentication step, their method provides the information about the specific frequency of the image that has been modified by the tampering action. The image authenticity validation in their method was performed using a validation key which comprises of inserted watermark, coefficient selection key and quantization parameter. The mother wavelet function was obligatory in their method for extraction or inserting the watermark. The visibility of the watermark in their approaches is controlled by the value of the maximum wavelet decomposition level. The quantization key provides the flexibility to make the technique more or less sensitive to certain distortions. The reported results of their method were also found promising.

A different image authentication scheme using watermarking approaches was proposed by Xiang Zhou et al (2004). In this method, the mark (sign) extracted from the original image is inserted as watermark for the authenticity process. It is similar to the digital signature based forgery detection techniques. This method is a type of quantization based active approaches. The usage of the watermark extracted from the image avoids the need of additional signature file in their method. In this method, in both watermark insertion and extraction procedure, a user private key was exploited. The key based insertion and extraction task increased the security of their approaches. This method was found to have the ability to detect the malicious

tamper made on the image and locate the tampered blocks in the image. The location of the tampered block aided in inferring the possible motive of the forgery, likely candidate adversaries, and equinity of the image. Moreover, the watermarking in this method consists of two parts, water mark and parity check bit (PCB). The parity check bit was utilized in their method to correct the extracted watermark because of lossy attacks. This procedure is called the Error correction coding. The watermark is extracted from the image based on some quantization step in a way that the receiver can detect the watermark without prior knowledge of the quantization step. The authentication was performed by comparing the pixels of the watermark image and watermark from the DWT coefficients.

Advantages:

- Water mark are designed in a way invisible human perception level
- Identification of manipulation over the spatial and frequency domain of the image is possible.
- Robust detection technique and More accurate

Disadvantages*:*

- Need special equipment for the insertion of the digital watermark onto the image.
- Prior information about the image is needed.
- Data modification without disturbing the lower significant bits of watermark code which contain the verification information seems problematic.
- Design of quantization key needs specific conceptualization to include the characterisation of geometric distortion.
- Explicit information about the tampering action is not provided. Needs prior information.
- Need more relevant feature extraction method.
- Vulnerable to incidental modifications.

2.2.2 Signature based detection techniques

In digital signature based techniques, set of features extracted from the image is used as the signature which is stored as a file and later on used for the authentication process. The significant characteristics of the signature based detection technique is that only the content of the image is utilized for authentication, whereas in watermark the content of the image is varied by the addition of the invisible information.

Ching-Yung Lin et al (1998) used digital signature for the detection of the forgery image. In this method, the authenticity of the image is verified using the digital signature authentication process. This method is a type of feature based active approaches. The significant advantage of their method was ability to detect the content changing manipulation such as pixel replacing tampering action and content preserving manipulation such as JPEG compression tampering action. In their method, the signature generation consists of two processing steps such as feature extraction and feature encryption. In feature extraction, some quantitative invariants or predictable properties of the images are extracted. Feature extraction process was carried out as follows; primarily the images are transformed into DCT coefficients, from which the feature codes are generated. Finally, they have encrypted the features codes with encryption using the public key encryption method. The signatures used in this apporach have the ability to survive JPEG compression as the content-based information included in the signatures is invariant before and after JPEG compression. Moreover, they have incorporated their approaches in a video authentication method and obtained promising results. The vast authentication of this method lead to a robust one independent of transcoding process and regardless of the format transformation between different compression standards (such as MPEG-1, MPEG-2, H.261 and H.263).

Marc Schneider et al (1998) investigated on a methodology for designing content based digital signature for image authentication. In this method, they have presented a continuous authenticity measure as the signature for the originality check. Normally, the signature was designed in such a way that the alteration in image because of lossy compression remains undetected. Other than the tampering action concerned with image modification, all other image manipulation is detected. In Lin, C.Y et al (1998), they aimed to develop a digital signature based forgery detection technique to protect the authenticity of the image as well as to enable the ability to survive acceptable compression. This method is a type of feature based active approaches. The major problem of their approaches is feature selection for the signature generation. Features such as edge information, colour or intensity histograms, DCT coefficients of the images were used for the signature generation. The feature which describes the content of the image is focussed more on their approaches. In this perspective, they have proposed a methodology for determination of the features set utilizing the histogram of the image. The histogram of the image does not contain the spatial information about the image intensities which is useful for signature generation. To include the image intensity, only the useful part of the histogram was considered by dividing the image into blocks separately. The Euclidean distance between intensity histograms was used as a measure of the content of the image for the signature generation. In this method, signature authentication was performed as; i) Content of the image is extracted using the feature function, ii) Data reduction using a hash function, iii) Hashed data is encrypted using the private key, iv) Decrypted using the public key and the features are compared with the author feature. The distance of the feature vectors greater than the threshold signifies as manipulated image.

Advantages:

- Digital signature can be used to authenticate the proof of first authorship.
- Protect the whole representation of the image, not the intended content of the image.

- Efficiently detect the image manipulation with the change of content
- Verify and authenticate the originality of the image with high robustness

Disadvantages:

- Need prior information of the image for the signature generation
- Protection against certain kind of manipulations only
- Restricted to certain type of image modification
- Inability to detect modification because of image compression which is desirable in most of the applications

2.3 Review of Passive approach based forgery detection

Passive approaches are the most expedient forgery detection technique. The passive approaches based forgery detection technique is also called the blind forgery detection. The blind name factor ascends because of the following fact that, passive approach only uses the received image for the originality check without any modification in image at the time of creation or capture. The passive approaches are adopted with the wellbeing assumption that the tampering action performed in the image affects the statistical property (inconsistency) of the image scene content which introduces new artifacts resulting in various forms of inconsistencies. By assessing these artifacts, the forgery is analysed in the passive approaches based detection techniques. The negligence of the prior information of the image makes it most popular in the current trends, where most of the pictures which are filed in for the authenticity are collected from the internet. Different types of the passive approaches are available based on the kind of forgery and the inconsistency twisted. An overview of the existing blind forgery techniques is reviewed in this section.

2.3.1 Copy-Move detection techniques

Copy move forgery is the most shared andstraight forward type of the image tampering technique. The tampering procedure in the copy move forgery is simple

because the original parts of the image are copied and moved to a desired location and pasted. The area duplication facilitates hiding certain details of the image. The part selected for the duplication is ordinarily the textured regions since it has the similar color and noise variation properties. Such belongings make the modifications unperceivable for the human eye. The literature of the existing research works related to the copy move forgery detection technique is given below.

Irene Amerini et al (2011) proposed an approaches for detecting the copy move image forgery using SIFT based method. In the main, to detect the copy move forgery, it is essential to recover the geometric information used to perform the duplication. This is because the forger can achieve the tampering target only by the application of the satisfactory geometric transformation. In this method, to detect the modifications made in the image a novel method based on scale invariant features transform was developed. The SIFT was used in this approaches to identify and describe the cluster points of the duplicated region. Upon the detection, the cluster points were used to reconstruct the geometric transformation parameters. In this method, they have detected the copy move tampering action using following steps; (i) Feature extraction- features allied with the correlation between the original image and duplicated area in the image were extracted primarily using SIFT, (ii) Feature matching process- The extracted features from the images were matched in the multiple key point matching process, (iii) Agglomerative clustering- matched points were clustered to identify the possible clones and verify whether the image is authentic or unauthentic. After authenticity verification, if the image is judged as non-authentic, the transformation parameters were estimated. The proposed methods have the ability to deal with the affine geometric transformations. The significant advantages of this apporach is the knack to individuate the altered area in the tampered image. They evaluated their method over ten tampered photos and the experimentation ensued in promising results. . Moreover, the geometric transformation parameters in the tampered image were estimated with high

reliability. They have also tested this method in the splicing attacks and obtained promising results.

Using multiresolution local pattern as the elementary, a method for detecting the copy move forgery detection was proposed by Reza Devarzani et al. (2013). This method focused more on the illumination variation rather than the geometric distortion for the duplicated region detection. The bossy benefit of this method was the capability to precisely detect the modified area in the image, with the robustness against the rotation, scaling, etc. Moreover, the proposed method covers the small and smooth forged area of the image as well. The disparity of this apporach over other copy move forgery detection techniques provided in the literature is the block based detection technique. Primarily, the image subjected to the originality check is divided into the overlapping blocks. Flowingly, the feature vectors from the image blocks were estimated using the Local Binary pattern Operator which has the ability to epitomize the statistical and textural characteristics of the images with low computational overhead. The LBP parameters were estimated by comparing the central pixel value of the image to the neighbourhood pixel which is assigned with some weighted powers and threshold. In the viewpoint of multiresolution LBP, they finished feature extraction through two, three and four types of the LBP operator. Afterwards, they have sorted the extracted feature vector in lexicographical order and then, they have utilized the block matching step where the K-d tree was used for matching the feature points to determine the duplicate image blocks. Consequently, they used the Random Sample Consensus algorithm for the determination of the geometric transformation parameters. In addition, the false matches were also removed by RANSAC. Accurate detection results were obtained in their experimentation with the individuality detection of modified even with distortion such as rotation, scaling, blurring, noise addition etc.

Region duplication forgery detection technique using wavelets transform and log polar mapping was introduced by A.N Myna et al. (2007). Illustrated detection

technique has used the wavelet transform for the dimensionality reduction of the image, thereby easing the detection procedure. The wavelet transform was used because of its ability to provide inherent multi resolution character of image. The detection was done in two phase, firstly exhaustive search for discovering the identical block is performed by log mapping polar function. Based on the log polar coordinates, a matrix value for each block is estimated and subsequent matching blocks is determined using the phase correlation as the similarity function. The block with the maximal phase correlation value greater than the threshold value was saved as matched blocks. Secondly, the saved blocks were compared at each level of wavelet transform which is nothing but the original image itself. Likewise, log polar mapping function was utilized and if the final set of correlation value obtained by the mapping function is found maximal, the image is considered fake. They have tested this method in various images with different block size and on image where the duplicated region is pasted with different angle of rotation. The major disadvantage of the illustrated method is application of exhaustive comparison for modification detection on the image only with lower resolution level. However, the computational cost for the mapping function created in this algorithm is improved. Favourable results were obtained in detecting modification in image of different format such as JPEG, BMP, PNG, etc.

The computational complexity of the copy move forgery detection techniques always seems knotty. Any assessment made to reduce the computational overhead, affects the performances of the detection. As a solution to this effect, Aaron Langille et al (2006) developed a method for detecting copy move forgery by an efficient match based method with low computational complexity. They aimed on duplication detection with reduced complexity by reducing the number of the matching operations. To detect the modification in the illustrated algorithm, firstly, the input image is segmented into blocks. The segmented blocks were sorted using k-dimensional tree. The k-d sorting technique groups the identical block closer to each other. Furthermore, in this method, the sorting procedure not only groups

identical blocks together but also the blocks with similar intensity patterns. The blocks sorted in the array were subjected to the matching technique. The k-d sorting process reduced the number of the matching operation required for the duplication detection. In matching, the similarity of the neighbouring blocks was estimated based on which the duplicated regions is detected. To increase the accuracy and reliability of the detection result, they have encoded the duplicate image into colour image and executed colour based morphology operations which removes the isolated mismatches and aids in filling the missing matches. The experimentation of this detection algorithm results in better detection accuracy but the limitation is concerned with the number of isolated mismatches which are possibly the matching blocks.

Advantage:

- Copy move forgery detection techniques can be extended to enumerate real data performance.
- Easier adaptation of matching technique improves the efficiency of detection
- Ability to detect modification in border regions of image

Disadvantage:

- Copy move forgery detection technique cannot be managed to detect all types of transformation
- Reliability of transformation parameter is not substantial
- Detection error may occur due to the quantization and interpolation error
- Computationally expensive
- Human interpretation is necessary
- Increased false rate
- Difficult to detect copy move tampering in image with small forged area

2.3.2 Splicing based detection techniques

Image splicing is another important and frequent type of forgery handled by the forgers for the image manipulation. In image splicing, the image fragments from one or more images are jointed into an original image creating false facts and evidence. The splicing forgery is commonly used because the effort required for modifying the image is minimal. Because of its simplicity, the image splicing detection is considered as the fundamental task of the image forgery detection. The splicing of the different image into the original image alters the correlation level which introduces new artifacts which can be used for detection. The literature of the existing research works related to the image splicing forgery detection is presented below.

Wei Zhang et al.(2010) obtained a splicing detection method based on the planar homography and graph cut method. The proposed method requires an automatic fake region detection method for identifying the splicing artifacts and fake region extraction method for localizing the forgery information. Illustrated detection technique used a planar homography constraint for detecting the fake region in the image which is specified as target. The target region contains the geometrical constraints which are responsible for the modification. Upon the target acquire, an extraction method was utilized to extract the fake objects from the manipulated image. They have used the graph cut segmentation method as the extraction method. Graph cut is one of the effective segmentation method which works on the principle of the maximum flow/minimum cut theory. To make the segmentation technique automatic, an online selection framework for different features and parameters was introduced. The selected function maximises the quality function of the graph cut thereby automating the segmentation procedure. Besides, the accuracy of the extracted fake objects was also increased by the online selection strategy. The experimentation of their method resulted in characterising the image manipulation with the stable and effective geometry based targeting and

improved graph cut segmentation method. They have tested this splicing detection technique over 5096 spliced images and obtained encouraging results. The limitation of this apporach is its inapplicability in picking up fake regions from large amount of the images. Moreover, the automatic graph cut segmentation method adopted in their detection technique is challenging because of the optimal feature and parameters online selection which are highly picture dependent. The performance of this apporach depends on the selection framework of the graph cut method which is not tolerable.

Image forgers perform splicing forgery in a certain colour space. In order to destroy the clue of forgery to the human perception level, they mean to cover all the manipulated traces in the image. By analysing the colour space, it is possible to detect the spliced image. A different splicing detection technique was introduced by Xudong Zhao et al. (2010) using Chroma colour space. Chroma space is also a colour space where the brightness is removed (luma). This method engrossed more on detecting the splicing forgery in the coloured images. The individuality of their method lifts of in the pre-processing step itself, where the image de-correlation is applied to reduce the unnecessary influence caused by the quiet image area in the image which reduces the computational overhead and searching time. The discontinuity in the spliced region posed by the splicing action is captured by the image de-correlation. In the illustrated process, Chroma space features are used for the separating the spliced images from the official pictures. Primarily, they have used pre-processing procedure followed by the feature extraction. The feature extraction technique employed in this method is Run Length Run Number (RLRL). They have extracted the features from every colour channels in all possible directions. The effectiveness of the Chroma based feature is analysed by performing the comparison over SVM classifier with the features of the RGB and luma. In this method, LIBSVM classifier with Radial Basis as kernel function was used with grid search parameterizing scheme. They have analysed the effectiveness of their method by experimenting over 800 authentic and 921 tampered images. The scatter

distribution of the spliced image with Chroma features was found with smaller overlap whereas luma features resulted in distribution with much overlap.

A natural image model based splicing detection was introduced by Yu.Q.Shi et al. (2007). The natural model developed in this method consists of different features of the image for the forgery detection. They have utilized the moment based features and marginal moment based features from the original test image and Markov based features from the 2-D array of the tested image. The combined feature scheme enabled in the proposed scheme provides promising splicing detection capability. The 2-D array of test image was constructed by the application of the Multi size block discrete cosine transform (MBDCT). MBDCT was employed because of its superior capability in de-correlation and energy compaction. The features generated by MBDCT 2-lyD significant increase the detection preface of this method. They mined the motion features from the test image by the application of the wavelet transform. Likewise, the Markov features were mined from the 2-D image by the application of the wavelet. The Markov based features reflects the demographic changes caused by the image manipulation. In order to reduce the dimension of the extracted features, a thresholding technique was also adopted. Combinational use of the two kinds of feature enhanced the effectiveness in splicing forgery detection. To signify the effectiveness of their method, they have featured a detailed implementation procedure on real dataset. The extract features were fed into a machine learning approaches for the decision making. For classifying the spliced image into authentic or unauthentic a SVM classifier is used in the illustrated detection algorithm. The experimentation of this method obtained promising results with the detection rate of 92%.

A unique methodology for detecting the splicing forgery was investigated by Pardhi et al.(2014). They aimed to reduce the user interaction in the decision making of the splicing detection. They demonstrated the splicing detection method with image involving the face of the people. A method was used to used identify the

illuminant map in the image. Upon illuminant detection, face detection of the image involving people was performed. Viola John detection method was used to detect the face region from the image. The image after the face detection was made in such a way with cropped face image. After the face detection, the features from the images were extracted from the cropped face image. In illustrated technique, the feature are extracted from the GLCM matrix. The statistical features such as energy, entropy, correlation sum of energy, the amount of correlation are calculated from the GLCM matrix. Also, the LBP features were also extracted. Besides, a new feature which provides the edge information of the spliced image was included by compelling the features HOGedge point which is based on the HOG descriptor. The extracted features were passed on to the classifier for the training. SVM is the classifier used in this method. In the testing, based on the trained features, the SVM classified the incoming image into authentic or unauthentic image. A crisp statement on the authenticity of spliced image was provided by this method.

Advantages:

- Requires minimal user interaction
- Easily adaptable to different feature extraction method and machine learning approaches
- Efficient method with low false positive
- Computationally less complex
- Flat regions of forgeries can be detected conveniently

Disadvantages:

- Unable to detect the splicing modification in pair of images with fake objects at perfect positions and in perfects shapes
- Impossible to detect manipulation in image with few feature points
- Infeasible for detecting spliced forgery in image with edge sharpness
- Minor tampering is difficult to detect

2.3.3 Image enhancement based detection techniques

Image enhancement based forgery detection technique is a distinctive detection methodology concerned with the detection of tampering action because of the image enhancement process. In general, the forgers tamper the image more imperceptible by including some image enhancement process such as resizing, resampling, rescaling, rotation, blurring etc. The enhancement operations performed on the image for the manipulation are often invisible tom human eye. But the image enhancement process introduces the specific correlation in the image which can be used as an evidence for the forgery detection. Figure 2.2 depicts three types of image enhancing process. Only three enhancement processes is signified in the literature since the research works related to the resampling, rescaling and blur based forgery detection technique appears to be more conversant.

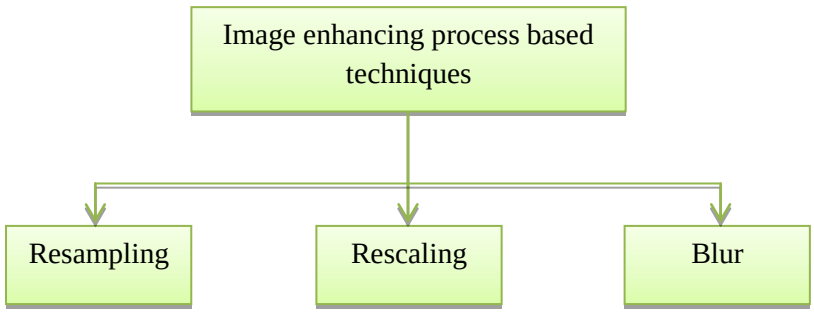

Figure.2.2 Types of image enhancing process

The literature of the existing research works related to the image enhancing process based forgery detection technique is given below.

(i) Resampling

Prasad S et al. (2006) implemented a forgery detection scheme based on characteristic change ensued in the image because of the resampling operations. Deterministic technique was utilized in this method to detect the correlation change.

Moreover; the tampered portion of the image is localized by this method. The presented deterministic technique comprises of different fouler techniques; Two for pixel domain and another two for frequency domain. The tampering was detected using the DCT high pass filtering and wavelets in frequency domain and using zero crossing function in pixel domain. Alin C. Popescu (2005) introduced a method which utilizes the periodic statistical properties of correlation caused by resampling for the tampering detection. The correlation in the image was detected using the EM algorithm. The probability map estimated by EM algorithm was analysed for composite detection. Similarly, in Popescu, A.C. and Farid, H(2004) a forgery detection technique exploiting the correlation caused by resampling was demonstrated by Farid et al. Several detection schemes have been poured on in this approaches for detecting the doctored image which is resized.

(ii) Rescaling

Weimin Wei et al. (2010) developed a method for estimating the forgery in the image because of the image rotation operation. The image rotation is nothing but the image scaling. In their method, periodicities in the interpolated image were exploited for the estimation of rotation angle. By analysing the interpolation induced spectral signatures of the images, the parameters of the scaling and rotation were determined. By the application of the estimated parameters, the fake objects inserted into the image were estimated. The proposed methods have the competency to find the forgery in image which is altered with multiple operations such as repeated zooming, rotation etc. They have analysed the proposed detection scheme over 100 forged images and obtained successive results.

(iii) Blurring

The degree of discontinuity or unwanted effects in the image is reduced by the blurring operation. Soo-Chang Pei et al. (2005) applied a method to detect the image forgery because of the blurring operation that involves global blur factor estimation. The blur estimation of the core image was done using the blur sharpness

threshold function. After blur estimation, the edges were removed and the consistency between defocus knowledge and blur estimation results was examined for the forgery detection. Similar blur estimation based tampering detection was demonstrated by Y.utcu et al.(2007). In this method, blur value of the image for the consistency check is estimated based on the regularity properties of the wavelet transform coefficients. S. Devi Mahalakshmi et al. (2012) proposed a method for image forgery detection that involves combined method for detecting the sharpness adjustment made in the image.

Map generation and transformation function were utilized for the blur value estimation. No time consuming iteration is involved in the detection process of the illustrated algorithm. A unique method with nearest neighbour and bilinear resampling factor estimation for detecting the image forgery because of blur operation was introduced by AriawanSuwendi et al. (2008). The adopted technique easily estimated the resampling factor because of interpolation. The experimentation of their method resulted in robust and reliable detection pattern.

Advantages:

- Simple and efficient
- Localization of tampered region is conceivable
- Reliable

Disadvantages:

- Human interpretation is necessary
- Increased false positive rate
- Efficient constraint estimation technique is necessary

2.3.4 Image format based detection techniques

Image format based detection technique utilizes the format variation of the image as the evidence for the tampering detection. On creation of forged image, the resultant image is inherent to different kind of compression artifacts based on the tampering source. The compression artifacts may be due to the recompression procedure. These compression artifacts results in variation in compression characteristics of the image which can be used to validate the image integrity. JPEG is the most export image file format used in most of the digital camera. The image processing operations applied for the tampering action affects the compression format ascending issues which is very essential in image tampering detection. The literature of the existing research works related to image format based forgery detection techniques are given below,

Tiziano Bianchi et al. (2012) developed a technique for detecting the image forgery based on image format. The detection was centred on examining the JPEG double compression. In order to test the presence or absence of the double compression atrifacts, they have used a unified statistical model which automatically computes the likelihood map of the DCT blocks of the image. But image pair with double compressed scenario was hard to detect. Another method centred on double compression artifacts as evidence for tampering detection was proposed by Piva et al (2012). Illustrated algorithm, only detect the nonaligned double JPEG (NA-JPEG) recompression. This method examines the DCT coefficient feature of the image. Simple threshold detector was used to classify the NA-JPEG images. The experimentation of their method resulted in superior results in terms of detection accuracy. Focused on the image artifacts due to the recompression, Yi-Lei Chen et al. (2012) proposed a new method for tampering detection. They have designed a robust detection approaches for discovering all the traces cause by the recompression of the images. The Periodic characteristic of the

JPEG image in spatial and transform domain was utilized to detect the block aligned and misaligned recompression.

Matthew C. Stamm et al. (2012) formulated an anti-forensic tool for compressed images. They originally intended this method for detecting the forgery in video but a special theoretical model was developed in their method significantly detected the compression artifacts. Moreover, they have introduced new game theoretic framework for evaluating the performance of the forgery operations. I-Cheng Chang et al. (2013) introduced a reliable method for the detection of the compressed images using multi region relation. Primarily, the suspicious region in the image was identified by searching the similarity blocks in an image. After the suspicious region discovery, the Multi Region relation was utilized to identify the forgery compressed images. They developed two stage searching algorithm to improve the sped of detection procedure. Andrew C. Gallagher (2005) created a interpolation detection algorithm. The significant advantage of this method is the ability to detect the presence of interpolation in image prior compression or after compression. Second derivative of the interpolated image was exploited for the forgery detection.

Advantages:

- Ability to work promptly
- Adaptation of synthesizing methods for detection of doctored images.
- Reliable

Disadvantages:

- Struggle in detecting the compression changes in graphic rendered images
- High false positive to natural image
- Validation of heavy compression image forgery is difficult

2.3.5 Camera based detection techniques

Camera based detection technique is one of the unique forgery detection technique. This detection technique is concerned with the imaging process using the camera. The digital camera consists of lens system, sampling filter, color filter array, colour interpolation and post processor. The processing in each of the individual elements of the camera varies from one another. In perspective of lens system, improper light focus during the capture embraces the correlation which can be used as evidence for tampering detection. Similarly, in imaging sensor, and CFA, the possibility for the inbound correlation is increasing which can be used as forgery evidence. Figure 2.3 depicts the different detection techniques in the camera imaging process well-thought-out in the literature.

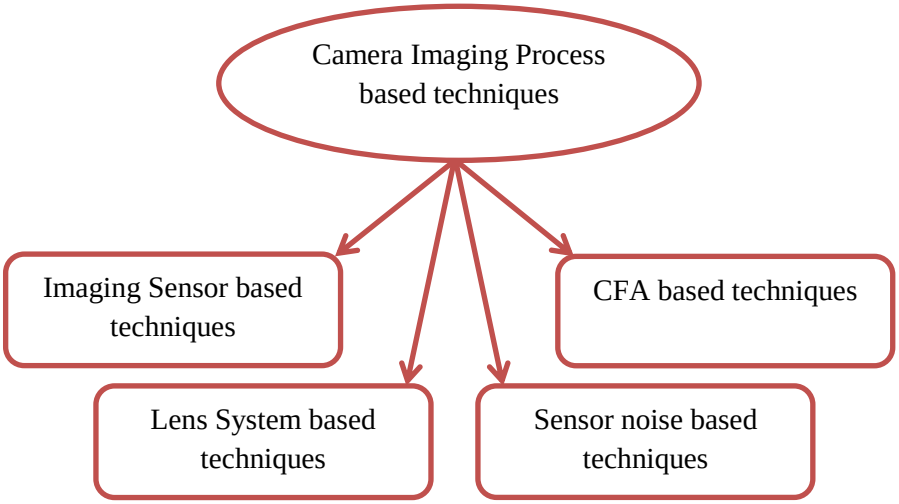

Figure.2.3 Types of detection techniques in Camera Imaging Process

The literature of the existing research works related to the camera imaging process based forgery detection technique is given below,

(a) Imaging sensor based techniques

AshwinSwaminathan et al. (2005) proposed a method for the image forensic analysis that involves the individual component visual sensor of the camera as tampering evidence. An analysis framework was developed in the illustrated detection scheme for analysing the visual sensor. The developed framework consists of set of forensic signal processing algorithm for estimation of the parameter variation because of sensor failures during the image acquisition process. The interpolation coefficient and CFA pattern of the camera were estimated for the forensic analysis. The experimentation of their method was performed over synthetic data set and camera data set. The trialling resulted in robust discovery of the visual sensor infringement problem.

(b) **Camera lens system based techniques**

The camera system consists of the optical lens system to focus the light for the image acquisition. The image forgery affects the chromatic aberration which can be used as evidence for the tampering detection. Micah K. Johnson et al. (2006) described a computational technique for estimating the lateral chromatic aberration of the image for the forgery detection. Primarily, the model for chromatic aberration was derived based on which the chromatic aberration value of the colour channel is estimated. The misalignment between the colour channels in chromatic aberration of the lens was used for the detection. In Swaminathan, A., et al. (2006), Ray Liu et al demonstrated a detection technique based on the inconsistencies of the camera lens system. In this method, the linear part of the tapering process was modelled as a filter and the coefficient were obtained using the blind convolution process. The obtained coefficients were matched for the forgery detection. Another passive forgery detection technique was demonstrated by the Xin Wang et al. (2008) in which the image patches of the defocus model is used for the composite detection. Generally, because of different imaging condition, the image patches with similar distance to the lens have similar blur kernel sizes. By analysing, the blur consistency of the edge of image patches, the forgery can be detected. In this view

point, they used a local blur estimation technique at each edge pixel to expose the blur inconsistency. The experimentation of their method obtained promising results. Another method of similar fashion which models the edge information of the image as a finite state Markov chain was proposed by We Wang et al. (2010).

(c) CFA based techniques

In camera, CFA is used to interpolate the missing colour samples to obtain three channel color image. This interpolation generates some specific correlation in the image which will be altered in the modification. Alin et al. (2005) introduced a method quantifying the specific correlation presented by the CFA interpolation for the forgery detection. A simple linear model was developed for detecting the CFA interpolation (in complicate case EM algorithm). NasirMemon et al (2005)also proposed a detection methodology based on CFA interpolation. In this method, based on the proprietary interpolation algorithm the source camera utilized for image acquisition was identified. Na fan et al. (2009) developed an authentication framework to recognise the DE mosaicing algorithm of camera CFA. A neural network framework was introduced in this method to detect the de-mosaicking algorithm with the assistance of the bias and weight adjustment. Upon the de-mosaicking algorithm detection, the modification in the image was estimated by analysing the algorithm of the source camera.

(d) Sensor noise based techniques

Jun Takamatsu et al. (2010)investigated on a forgery detection algorithm that involves the estimation of the demosicing algorithm of the camera using the image noise variance. The noise variance was introduced because of the visual Ensor. The spatial variation of the image noise variance was utilized in this method to detect the de-mosaicking algorithm of the CFA based on which the tapering action is detected. Another image integrity determination method using the sensor noise was proposed by Mo Chen et al. (2008). In this method, the doctored images are revealed using the photo response non uniformity noise (PRNU) of the imaging

sensor. Maximum likelihood estimator was used to obtain the PRNU from the sensor output. The detected PRNY was analysed for the prediction authenticity check. Moreover, the source digital camera was also identified by the framework adopted in this method. Similar approaches was also proposed by Chung Hsu et al. in (2008)in which Gaussian Mixture Model was utilized to model the distribution of the correlation of temporal noise residue.

Advantages:

- Reliable exposure of forgery
- Accurate detection
- Enhanced performance over low quality image

Disadvantages:

- Limitation in rendering any type of image forgery
- Misclassification rate is high
- Detection accuracy lowers when handling compressed images
- Difficulty to find corrupted region with small noise degradation
- Increased computation time

2.3.6 Shadow based detection techniques

Shadow based detection technique is relevant to the physics based passive approaches (as mentioned in section 1.5.2 of chapter 1. In the image manipulation process, geometric transformations are given to the image to give the impression that the image is authentic. The transformation include enhancement process, modification process etc. However, shadow in an image is inevitable. The geometric transformation concerned with the image manipulation in regard to the shadow is left overlook by the forgers. This shadow inconsistency can be used as an evidence for the tampering detection. Shadow based detection technique is attractive compared to other detection techniques because the modification of the

shadow present in the image is difficult to attain. Moreover, shadows survive common compression operation performed for manipulation. The literature of the existing research works related to the shadow based detection technique is given below,

YongzhenKe et al. (2014) investigated a method to detect the image composites by imposing the geometric constraints from the shadow inconsistency of the image. In particular, the authors explored the suspicion region of the image including shadow and non-shadow. Illustrated method, mainly concentrated on the image with inconsistent shadow because of the splicing operation. They reached the goal of image composite exposure by comparing the features of the image regions with and without shadow. Primarily, suspicious region from the image was manually selected and masked to separate the shadow and non-shadow region. Consequently, the texture feature of the shadow and non-shadow region (inside and outside) were extracted. In this method, Local Binary Pattern was adopted as feature extractor because of its practical significance. The extracted features were then compared using correlation similarity function and the tampered images are estimated. Moreover, they have introduced a different technique acceptable for detecting any type of forgery in which the strength of the light source was estimated from the image and compared by the correlation function for the detection. The experimentation of their method resulted in forgery detection with enhanced detection accuracy.

Another shadow based detection method utilizing the shading and shadow inconsistency was introduced by the Eric Keeet al. (2014). They used the physical inconsistency in lighting from the shading as well as shading as the forgery evidence. This method differs from preceding method for the reason of combined consideration of shading and shadow. The significant advantage of this method is related to assumptions made on the scene geometry. In the illustrated method, the multitude of shading and shadows based constraint were estimated on the projected

location of a distance point light source. Shading constraint from the 2-D and 3-D direction of distinct point light was estimated separately. The estimated constraints were formerly combined with a linear framework to determine the consistency of the shadow and shading with single light source. The consistency deliberates the originality of the image. Moreover, with the combined multiple shadow constraint, they have checked the possibility in consistency detection. This method obtained promising results in visually compelling forgery images.

James O'Brien et al. (2013) proposed a different technique for exposing the image manipulation using the inconsistent shadow. A geometric technique was adopted in their method to describe the cast and attached shadows which restrict the projection of the light source. A cast shadow is the wedge shaped constraints which doesn't occlude the object from themselves and the attached shadows are the shadow which occlude the object from themselves. In both the cast and attached shadows, the correspondence between the points in and out of a shadow on either side of the objects is similar. After determining the shadow constraints, they are framed as a linear programming model. The consistency of the image is identified based on the linear programming problem. Moreover, they have described a simple randomized algorithm for the finding the approximal set of the conflicting constraints that identifies the inconsistent shadows. The effectiveness of this method depends on the number of the constraint considered for the consistency check and the consideration of the cast and attached shadow. Linear programming model provided computationally efficient solution. The limitation of this approaches is concerned with the single light source assumption.

Bin Yang et al. (2015) investigated a method for detecting the photographic splicing using shadow inconsistency. The processing steps involved in this method are; i) Shadow boundary extraction, ii) Shadow Scale factor estimation, iii) Shadow growth rate estimation, and iv) forgery detection. Shadow boundary was extracted from the image with the provision of the SVM classifier and user interaction.

Shadow scale factors were estimated from the shadow boundaries using energy minimization approximation. The shadow scale factors of the textures surfaces were given more important. Shadow growth rate in terms of penumbera width (GRPW) was estimated with the help of Markov Random Filed technique. Forgery detection was performed by taking in the scaling factors along with GRPW of the distinctive colour channels of the image. The difference in shadow vectors, proved the originality of the image. They have analysed their technique on real images and forgery images. The proposed method also proved the robustness in detecting the image with forgery operations related to compression and noise addition.

Another image composite authentication method based on single shadow observation was proposed by CAO XiaoChun et al. (2015). The relaxation in the shadow observation requirement is the imperative advantage of this method. The sun elevation was adapted as the cue for the authenticity check in their method. The Sun elevation of the ground truth image was estimated using the EXIF information (Exchangeable Image file). The Sun elevation of the image was estimated base on the geometric constraints. By comparing the sun elevation, the image forgery was exposed. They have analysed the proposed method on both the synthetic data and visually plausible image and obtained superior performance.

2.3.7 Reflection based detection techniques

Reflection based detection technique is related to the geometry based passive approaches (as mentioned in section 1.5.2 of chapter 1). When altering an image, in order to conceal the traces of the forgery various processing operations are performed, but it is often difficult to exactly match the reflections of the objects present in the image content. The diffusive reflection of the object can be compelled at the first glance however at close examination the reflection inconsistency can be discovered. The inconsistency in the reflection can be used as an evidence for the tampering detection. The inconsistency in shadow can be analysed by estimating the

direction of the light source. Like shadow based detection technique, reflection based detection technique is also a favourable forgery detection technique. The literature of the existing research works related to the reflection based forgery detection technique is given below,

James F. O'Brien et al (2012) described a method for exposing the image manipulation using the inconsistent reflection in the image. The geometric inconsistencies ascend in the manipulated image at time when the forger tries to insert the fake reflection of the object in the image scene content. By analysing this geometric inconsistency, the tampering action performed over the original image can be detected and localized. They have used the basic rules of the reflective geometry, and linear perspective projection for the reflection analysis. In the illustrated detection technique, for attaining the reflection information some minimal assumptions are made about the image scene geometry. Primarily, they tried to obtain the underlying geometric relation in the image by combining the 3-D geometric relation of planar reflection with the geometry of linear perspective projection. The reflection vanishing points alongside the orthogonal direction of the objects, reflection line midpoints and centre of projection point, implausible midpoints corresponding to the feature points of the image were estimated. After the detection of the reflection point concerned with different constraints, inconsistencies were detected by comparing the reflection point and the object feature point. The significant advantage of their method is the ability to expose the forgery in image insensitive to common processing operations such as resampling, colour manipulations, lossy compression etc.

Another image forgery detection method using the inconsistent reflection vanishing point was described by Huayongge et al. in (2014). They aimed to reduce the appropriate feature selection problem which raises the uncertainty in large error distance of reflection vanishing point. In this method, Sin2() based function was used to normalize the error distance. Moreover, the maximal normalized error

distance was utilized to expose the image forgery. In this method, initially, the reflection vanishing points of the objects in the seen was estimated directly or indirectly of the planar reflection. The error distance between the reflection point intersections is measured. The dispersion of the intersection scattering is much larger for the forged image and smaller for the authentic image. To exploit the forgery, the maximum error distance from the intersection scattering was found and analysed. They have tested the accuracy and effectiveness of the proposed technique over a dataset consisting of 200 authentic and forged images. The experimentation resulted in promising results. The normalized error distance of the forged images were found larger and the normalized error distance of the authentic images were found minimal.

Micah. K. Johnson et al. (2005) demonstrated an image forgery detection using the inconsistencies in the lighting. The lighting inconsistency also causes the reflection in significantly different position. In this method, the direction of the light source responsible for the reflection of the object in the image cane content was estimated and the inconsistencies in the light direct was used up for detecting the tampering action. They have made some assumptions for the estimation of the light source such as i) Surface of interest reflects the light isotropically with constant reflectance value ii) The surface of interest is illuminated by a point light source and iii) The angle between the surface normal and the direction of the light is in the range zero and ninety degree. In their method, the localisation of the boundary in the image was obtained by manually selecting the points alongside the image. The intensity of the occluding boundary is the place where the light source direction is estimated. By comparing the reflectance of the object across the boundary, the forgery was exposed.

HanyFarid et al. (2007) introduced a new digital image forgery detection technique by taking the lighting inconsistency as evidence. They used the statistic that at the time of the creation, lighting condition matching process is difficult to

attain as the basics for the tampering detection. Primarily, they aimed to model the light environments with the assumptions that the surface reflectance is constant and camera response is linear. From irradiance to intensity, all the light reaching point in the surface was estimated for the exposing purpose based on which the lighting environment was determined. From the lighting environment model, the coefficient vectors were estimated which is nothing but the model parameters. The coefficient of the objects in the different lighting environment should be distinguishable and the coefficient of objects from the same lighting environment should be similar. In this method, the difference between the lighting environments based upon the coefficient value is matched and analysed for the forgery exposure. For different colour channels, the light environment coefficients were estimated distinctly. However, the precise matching of the lighting of an image always seems difficult.

Advantages:

- Possible to detect any type of image forgery because the traces of the inconsistencies in reflection are difficult to hide
- Detection performance is superior on low quality images
- Semiautomatic method

Disadvantages:

- It is not possible to create the correct reflection to support the desired fiction of the image.
- Passable reflection may alter the detection accuracy
- Accurate selection of feature is necessary
- Handling multiple features is difficult
- Vulnerable to counter measures

2.4 Image processing techniques for image shadow and reflection detection

To detect the manipulated image composite with geometric inconsistencies of shadow or reflection, the discovery of the shadow/reflection region is requisite. In general, many of the image processing techniques is applied to the image for the separating the image and mesh data Kang, G., (1977). Image processing is a technique in which the images are processed using mathematical operations using any form of the signal processing. The processing output is either image or a set of characteristics or parameters regarding the image which embraces the mesh data. Segmentation is an important technique used in image processing to identify the objects in the image. Based on the object discovery, the image analysis can be done. By adopting the segmentation technique in shadow or reflection based detection technique, the unstructured shadow/reflection region from the image can be effortlessly separated for the analysis Jian Li et al.(2014).

Image segmentation technique is accepted as an applicative task in most of the image science field. In the image forgery detection, the segmentation is applied to extract the inconsistent region from the image based on which the features are extracted, matched and analysed to validate the image originality. The block diagram of segmentation based shadow and reflection detection is depicted in figure 2.4. Figure 2.4 epitomize the common flow of the segmentation adopted shadow or reflection based forgery detection. Primarily, the image subjected to the originality validation is subjected to any pre-processing procedures (if necessary). Subsequently, image processing operation segmentation is applied on to the accepted input image. Image segmentation partitions the digital image into multiple segments. In the view point of shadow or reflection based forgery detection technique, the analysis will be made ease only after separating the shadow or reflected region from the image which is provided by segmentation.

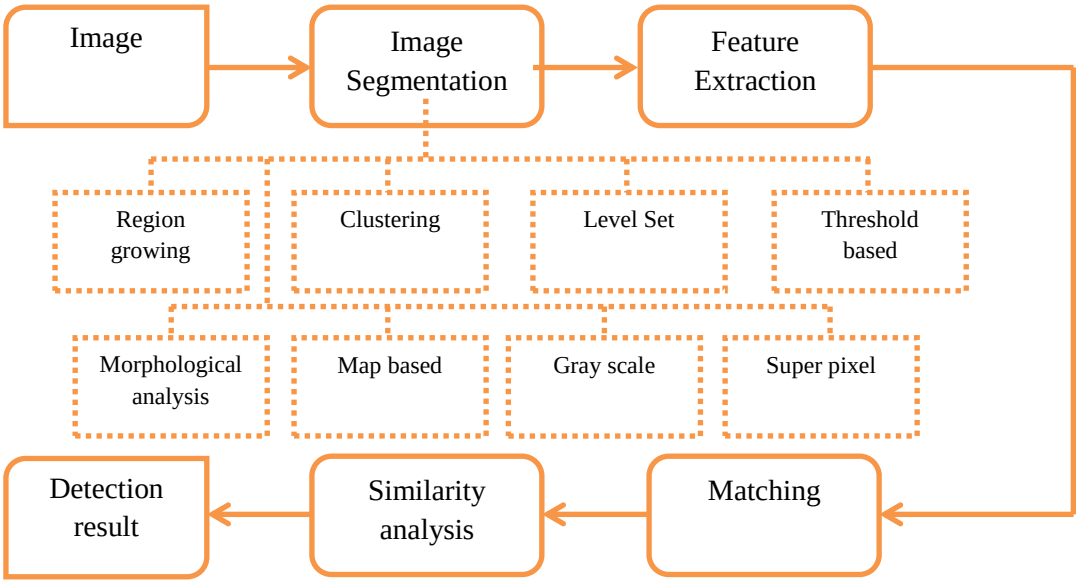

Figure2.4 Segmentation technique based Shadow and Reflection detection

The segmentation result in addition to the shadow or reflected region covers the whole image, in this manner analysing the characteristics of the segmented shadow/reflection region, the image composition can be detected. The analysis will be of affluence because of the individuality of pixel characteristics in the inconsistent region as well as the consistent region. As a whole, many of the image segmentation techniques are available. The effectiveness of the image segmentation depends on the domain knowledge on which the technique is applied. In the segmentation based shadow or reflection detection, many of the segmentation technique are adopted. They are

- Region growing based segmentation
- Clustering based segmentation
- Level set segmentation
- Thresholding based segmentation
- Morphological analysis based segmentation
- Map based segmentation
- Gray scale segmentation

The adopted segmentation technique segments the shadow or reflection region from the image. From the separated region, the feature points are extracted. The extracted feature points are matched and similarity of the reflection/shadow point extracted from the region is analysed. Based on the similarity, the integrity of the image is patterned. In some detection techniques, instead of feature extraction, the shadow/reflection points of the image is estimated using geometry technique and the estimated inconsistency point is compared with shadow and reflection points from the separated region of the segmentation result and the originality is analysed.

2.5 Machine learning technique for image shadow and reflection detection

Artificial intelligence is a ‘state of art’ problem solving entity used in any field associated with the computer vision. Machine learning technique is a type of artificial intelligence with the ability to learn without being explicitly programmed and predict or classify based on the learned data Carbonell, J.G., et al.(1983). Thorough data analysis is feasibly provided by the machine learning techniques. In image forgery detection, machine learning technique is used for validating the image authenticity. This is because of the composite nature of the objects in the scene content. In the view point shadow/reflection based forgery detection, the practice of machine learning technique is indispensible. The learning based detection approaches improves the detection performance of the adapted detection scheme. Some of the significant advantage of the machine learning based techniques are) knack to solve many real world problem ii) ability to classify the database with incomplete information. These advantages are obligatory in the image forgery detection.

Machine learning technique is accepted as one of the main stays in the image forgery detection. The block diagram of the machine learning technique for shadow and reflection based forgery detection technique is shown in figure 3.1. Primarily,

the image accepted for the originality check is subjected to the image segmentation. In image segmentation step, the shadow/reflection region of the image is segmented using any of the segmentation technique (as discussed in chapter 2). After region separation, the feature points are extracted from the corresponding shadow or reflection region. The features more concerned with the image texture, light strength etc. are extracted. Such features are extracted because only those have the bursting association with shadow/ reflection inconsistency. After the feature extraction, the feature points are fed to the machine learning technique.

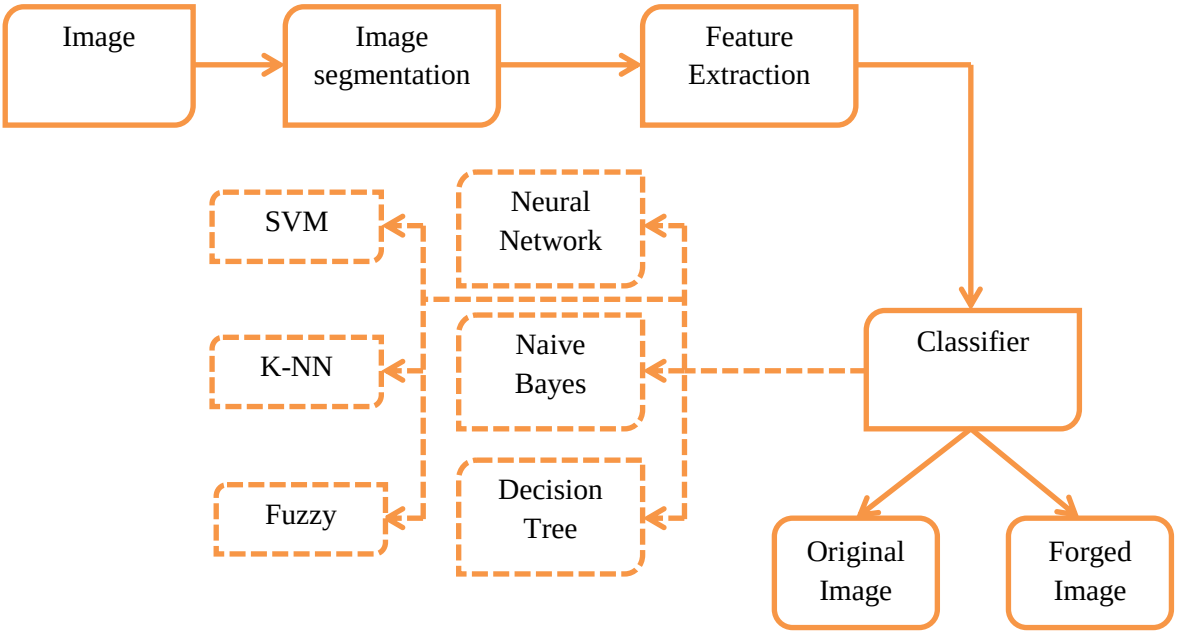

Figure.2.5 Machine learning technique based shadow and reflection detection technique

For the classification procedure of the image subjected to originality check into genuine or fake image, various types of the machine learning classifiers are used. The machine learning classifier used for the shadow/ reflection based detection techniques include;

- SVM classifier
- k-NN classifier
- Fuzzy set based classifier
- Naive Bayes classifier:
- Decision Tree classifier
- Naive Bayes classifier

The machine learning classifies the input image into fake or original one. In machine learning, the classification is performed in two phases i.e. training phase and testing phase.

In training phase, the classifier is trained with the extracted image features of the separated shadow or reflection region. In the testing phase/classification phase, the image from the database is subjected directly to the classifier which based on the learned data predicts the originality of the image. The machine learning technique is often used in the recent trends of the image forgery detection because of the improved detection performance.

2.6 Summary

The requisite for the image forgery detection is increasing to reimburse the forgeries introduced in the modern world. A survey has been made to identify the research articles concerned with the forgery detection. Based on the type of forgery performed, literature has been provided in this chapter. At first, the active approaches based forgery detection techniques such as watermark and digital signature techniques are discussed highlighting the advantages and disadvantages, as per the literature the prior knowledge requirement makes the active approaches unfeasible for practical cases. Secondly, the passive approaches based detection techniques such as copy move detection, splicing detection, Image enhancement detection, image format detection, camera imaging detection, shadow detection and reflection detection techniques are discussed with explicit remark on the advantages

and shortcomings. As per the literature, the blind approaches with ability to detect the originality of the image modified with any type of forgery seems necessary. It also describes the segmentation methods for separating the shadow or reflection region from the image for the forgery detection and the machine learning techniques for the shadow or reflection based forgery detection is summarized.