CHAPTER 1

INTRODUCTION

Immense innovations are made day by day in the current technical era. From the history, it is found that images are the most reliable medium for information transfer. There is an old saying confirming this fact that “A picture is worth a thousand words”. From the preceding history till now, the visual representation is the most common way utilized for expressing and transmitting information. Images are considered imperative since information which needs thousands of words for expressing the intended stuff can be uttered with a single image. The images are instantaneous and their content is easily understood which is granted than the texts which brands it as an effective one for the human communication Baxes, G. A.,(1994). For example, consider the share market, over time the share varies, for the analysis, in words it may takes years to understand the loss and gain rate, instead with the help of the images it can be known in minutes. This may not sound effective, but it is noteworthy. The practice of the image as the information medium is human nature itself, i.e. the information retrieval capability of the visual system from the image is extremely faster than another kind of information.

In early years, film photography and the darkroom where found to be the answer for the visual representation Guillon, J. P.,(1982), but now the thing is contradictory. Digital images took its place in existence of the film photography with pluses Van Dijck, J.,(2008). Moreover, unlike conventional photography, the image capture by the digital cameras is easy, besides the storage and transfer is also feasible. In the current information era, the benefits of the digital images are exploited in different filed such as military, news, media, medical diagnosis, forensics, tabloid magazines, scientific journals, fashion industries, court halls and so on Watson, A. B., & Null, C. H.,(1997) One of the central filed which fetched a notable gain is electronic commerce (Amazon, Snap deal etc.). Because of the

advancement in IT and internet sector, the growth rate in E-Commerce has considerably increased in the recent years. In electronic commerce, the products are showcased with the images for the users and the users retail the online purchase only based on the image certainty, as per the world internet statistics, a growth rate of 160% has been reported in electronic commerce sector from 2000-2005. Currently, 50 million internet users have made an online retail purchase. For every year, the cohort is expected to grow 100 million users. With the wide spread use of the internet, and availability of the different types of camera which are affordable at low prices, digital images is considered a major source of information in today's digital world Brinkmann, R.,(1999).

Fundamentally image comprises of series of pixels. Pixels name factor is an attractive one i.e. it is derived by combining the pictures and elements Sachs, J.,(1999).The digital image is generated by colouring the individual pixels of the images. A digital image is nothing but a slew of pixel set in some logical state. The digital colour images are represented by 8 bit numbers. In the number depiction, each of the octets corresponds to the amount of the red, green and blue pixels encompassed with in the image. The images are classified based on the format they are chosen for the storage. The format variation is for application orientated environment. Some of the format of the images is BMP, TIFF, JPEG etc. The image formats such as BMP, TIFF are used in lossless compression scheme. Such formats do not discard any information in the compression process which improves the quality of the image Sturak, J.,(2004).

The significant advantage of the digital image is they do not deteriorate from the time of capture. The progress in digital photography in the recent decades amplified the use of pictorial information and has become easier due to advances in digital photography Minakshi, K.,(2003). Today, almost everybody can record, store and share a large amount of digital images because of the spread of easy and cost effective device that enables the acquisition of visual data Shivakumar, B. and

Baboo, S.,(2011). The mobile phone camera is becoming very familiar and we know the impact of it in day to day life. But the question ascends with this growing world, where malicious attacks are made in every possible filed, is it acceptable to believe which is seen. The surety to check whether the image is original is obligatory. The authenticity of the image is important since it is the information.

1.1 Image Forgery

With the technical evolution the world is conquering, the trust on the digital imaging technology is grinding down. In daily life, peoples come across the tampered or forged images from the tabloid magazines to the business industry. Furthermore in media outlets, scientific journals, political campaigns, courtrooms, and photo hoaxes that land in our email boxes, forged images are appearing more frequently in a unique way unable to identify the fake image with the needed sophistication. The nominal advancement from the film photography to digital photography is feasible boon but it is not trustworthy. Conventional film photographs can't be edited whereas the digital images can be edited and modified after the capture. Conversely, with encouragements of the today's computer technology, more sophisticated software's like Adobe Photoshop , Corel Draw or Gimp are available for the modification of the original images, resulting in image tampering. Image forgery has a long history Rocha A, et al (2011). The image tampering in the perspective of digital works can be considered as a creative work but there are some cases where the tampered images are being maliciously abused. Such critical condition arises where images seems to be the proof for the medical reports, crime scenes etc. where the forged image results in patients death and escape of the criminal respectively. The forging of the original image leads to illicit distribution, which raises the data famine problem. In research filed, the data owners are cautious about publishing their images without ownership and copyright which reduced the data availability for the researchers. Likewise, many problems

arose in different fields because of the image forging. Some of the recognized examples of the image forgery are listed below;

- As per the survey conducted by the Wall Street Journal, in the USA 10% of the color photographs published in the magazines, newspapers etc. are digitally altered and retouched Amsberry C., (1989).

- In Farid H.,(2006) Pearson H.,(2005), scientific community has also been subjected to the image forgeries. Here, the result of a research work is retouched and reused by a different researcher leading to patent problem.

Authenticity and integrity of the digital images are well-thought-out to be important to overcome these issues because of the forging in fields such as forensic, medical imaging, e-commerce, industrial photography, etc. The authenticity verification check of the image is popularly used where the images are considered to supporting evidences, historical records, insurance claims, etc. Because of the drastic increase in the software availability for the advanced image manipulation and processing, the original images are tampered i.e. altered and modified without leaving any trace for forgery detection. This results in revising the old saying "A picture is worth a thousand words" to "A picture unworthy a thousand true words".

Definitions:

- "The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity", A. C. Popescu and H. Farid,(2004).

- "With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media", A. C. Popescu and H. Farid,(2004).

1.1.1 Problems to Detect Image Forgery

The major problems contained within for the detection of the image forgery are

- **Data Provenance**

Data source is the initial problem in the forgery detection. Vast number of images are available on the internet, in order to detect the forgery, the source of the original image is needed for the protection of rights and may be for supervisory prerequisite in applications like science, medicine, financial transactions government legal prosecutions and many more daily situations, wherever the information is valuable and trustworthy.

- **Benchmarking and Standard data set**

The need for open data set for critical realisation of forging seems another problem in image forgery detection. The unavailability of the images in uncompressed form with different resolutions, sizes and image acquisition model with diverse contents are some of the needed image conditions for detecting the fake image from the original image which is critical to obtain.

- **Duplicate Regions**

Duplication region appearance in the original image with same size, shape and colour appears to be another problem to detect the image forgery.

1.1.2 Digital Image Forensic

In the preceding years, the field of digital forensics has emerged to help restore the trust of the image by proper authentication process. Digital forensic is a branch of science which deals with image forgery. The ultimate intent is to reconstruct the events of the forged images and to identify the entities involved in it. The originality and reliability of the digital images are major concern of the image

forensic field. In diverse outlook, forensic is the application of scientific approaches for the detection and investigation of crime. Such forensic analysis serves in providing proof or evidence at courts. Recently, Digital images have widely spread leading to the use of digital image forensic in broader context of situation Kirchner, M.,(2012). The tasks involved in the digital image forensics are

1) Source classification
2) Device identification
3) Device linking groups
4) Processing history recovery
5) Forgery detection
6) Anomaly investigation

In source classification task, the objective is to classify the forged images based on their origin. For example image captured from the scans vs. digital camera images, canon vs. Kodak images etc. are classified individually. Device identification task is to identify the specific device using which the image is captured. Device linking group task is used to identify the images taken from the same source camera. In processing history recovery task, the processing chain applied to the images such as lossy compression, filtering, resizing etc. are identified. In forgery detection, the malicious processing in the fake image is verified. Anomaly investigation is concerned with the explanation of anomalies found in the tampered images.

1.2 Types of Image Forgery

The semantic information of an image is altered by addition or extracting information from the image. In order to achieve the image forging, numerous ways are used by the forgers. In general, there exist different types of the image forgery. The categorization of the types of image forgery is a tedious task; this is because the

forgery types are grouped based on the process involved creating the fake image. But in the current technical world, new innovations are made in the digital photography, which ascend new malicious forging techniques day by day. However, based on the existing types, a categorization is made in this research explaining different types of the image forgery Thajeel, S. and Sulong, G.,(2014). Figure 1.1 depicts the different types of image forgery.

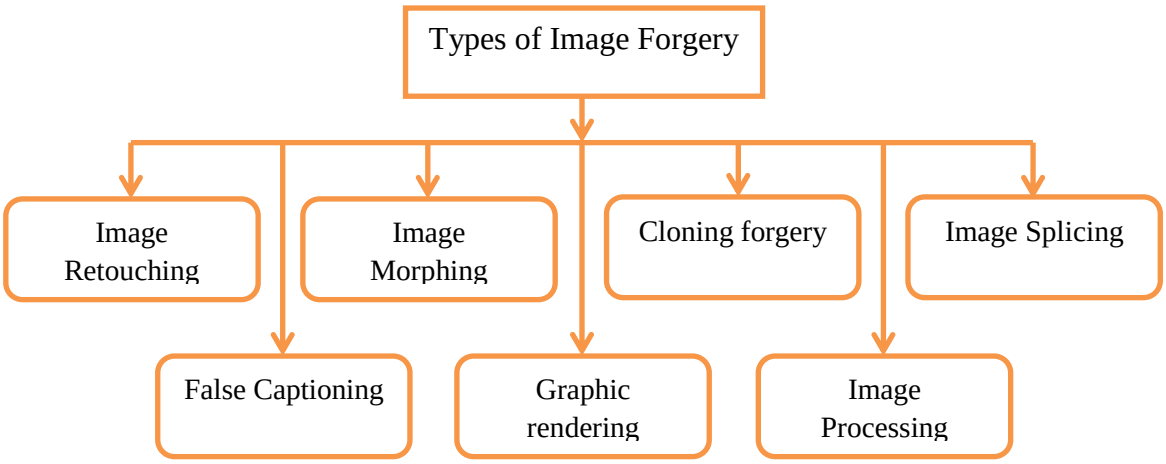


Figure.1.1 Types of Image Forgery

1.2.1 Image Retouching

Image retouching is one of the less harmful digital image forgery techniques. It is said so because it doesn't alter the visual messages of an image Al-Hammadi M.,. Image editing is the main mechanism in image retouching. In this method, the images are edited with different background, attractive colours, and work with the hue saturation for toning and balancing the image is performed. It is used to enhance the image quality to capture the reader's attention. Now a day, the image retouching forgery is familiar in social media like Facebook, Twitter etc., where the users post their retouched image by addition of filtering, etc. to acquire more favourites (likes) for the image Al-Hammadi M., Shah, H. Shinde, P,(2013).

1.2.2 Image morphing

Image morphing is a different type of forgery. In this method, the original image is transformed into another image by smooth transition of images Shah, H. Shinde, P. Kukreja, J,(2013). An example for morphing is available in xmorph.sourceforge.net. The image forging type forgery is critical nowadays leading to scandals etc.

1.2.3 Splicing

Splicing is dissimilar types of image forgery. In this method, different elements from multiple images are placed in a single image altering the image reality ChitwanBhallaSurbhi Gupta,(2016). It is also called as composition or photomontage. Spliced images are considered to be harmful because of the reality damage.

1.2.4 Copy paste

Copy paste forgery is considered to be the most common type of the image forgery. In this method, the regions from the original images are copied and pasted within the same image Sridevi, M et al (2012). In certain cases, the images are pasted within with possible transformation Amerini, I et al (2013). The region duplication is the main intend of the copy paste forgery. The copy paste forgery is also called a copy move forgery or region duplication forgery or cloning. The copy move forgery is realised into different types based on the way on which the duplicated region is pasted in the original image. They are

1) Copy move with rotation
2) Copy move with a different scale
3) Copy move with reflection etc.

1.2.5 Image processing

Image processing based forgery is another type of image forgery. It does not fall within the traditional definition of the image tampering, since there is no hiding or adding of the information Farid, H.,(2009) Birajdar, G. K., &Mankar, V. H.,(2013). It seems similar to the image retouching, however slight variations are present. In retouching, the background of the image is forged, whereas in image processing the whole part of the image is forged. The reality of the original image is altered at a psychological level in the image processing based techniques. Several categories of the image processing forgery are available. The subsection lists the different types of image processing forgery;

Scaling:

In scaling forgery, the scale of the object in the original image is altered. For example, an African person (black) is tampered onto English person (white) by altering the image. The scale forgery also induces malicious abuses in political propaganda.

Contrast:

In contrast forgery, the objects of the image (e.g., face) are highlighted more photo realistic using luminosity nonlinearity technique Granty, R et al (2010). This highlight is achieved by varying the contrast, brightness and window level of the image. In some cases, the luminance filters like radial glow, gradient glow, etc. are applied.

Resampling:

Resampling forgery is also called the resizing forgery. It is common in composite which needed for convincing the sustaining facts M. Kirchner (2008). It is used to shrink or enlarge the size of an image or part of an image. It may give the impression that the image is original as the size is enlarged. But while resizing the image, the certain unnatural correlations between the neighbouring pixels are

detected increasing the possibility of the tampering in the image M. Kirchner,(2010) A. Popescu and H. Farid (2005).

Cropping:

Cropping forgery is done to cut off the border of an image displayed. Generally, the border information is strange, however in certain cases it seems adequate Luo, W et al (2007).

Graphic rendering:

In this type of forgery, the images are tampered using different computer based graphic rendering tools to make look those sorts of more superficial Gallagher, A. C., & Chen, T.,(2008).

1.2.6 False captioning

False captioning is a changeless type of image forgery. In this method, the image is kept untouched, but the caption of the image is falsely inserted changing the actual information image misleading the viewer or reader Sangwon Lee et al (2006). In this method, the content of image is untouched while tampering the context of the image. This is the false captioning forgery.

1.2.7 Examples of Image Forgery

Some of the examples of the different type of the forgery are presented in this section. Figure 1.2 depicts the example of image retouching forgery. Figure 1.2a represents the fake image and figure 1.2b represents the original image. Here, the background of the original image containing cracks is retouched with a better background.

(a) Fake Image | (b) Original Image

Figure.1.2 Image retouching forgery

Figure 1.3 signifies the example for image processing forgery. Figure 1.3b represents the original satellite image of India which is manipulated as coloured image shown in figure 1.3a using image processing forgery.

(a) Fake Image | **(b)** Original Image

Figure.1.3 Image Processing Forgery

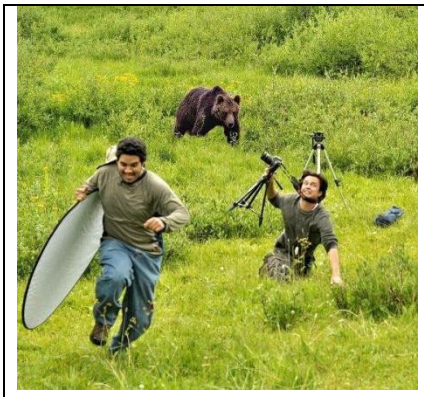
Figure 1.4 epitomizes the contrast forgery. Figure 1.4b depicts the original image captured during late 90's car festival which is manipulated into coloured image by enhancing the contrast of the image as shown in figure 1.4a.

(a) Fake Image

(b) Original Image

Figure.1.4 Contrast Forgery

An example for splicing forgery is shown in figure 1.5. Figure 1.5a represents the spliced image which is considered an impactful image of the national geographic crew which is later proved to be the fake one. The bear in the fake image is the stock photo which is identified by the grass in front of bear's leg.



(a) Fake Image

(b) Cut-paste image

Figure.1.5 Splicing Forgery

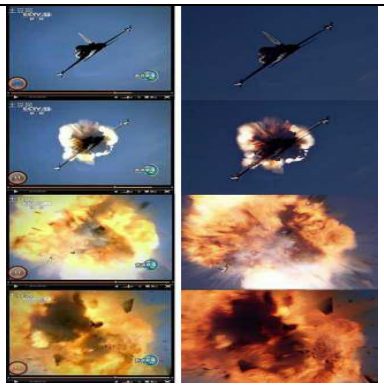
Figure 1.6 depicts the image morphing forgery. Figure 1.6a depicts the fake image which is created by morphing the original image shown in figure 1.6b.Tthe morphing is completed by the facial transition.

(a) Fake Image

(b) Original Image

Figure.1.6 Image morphing forgery

An example for false captioning forgery is depicted in figure 1.7. This image is broadcasted by the Chinese media as air force training procedure and failure. Later on, it was found to be the image taken from the movie top gun. The image is unaltered but the context caption is falsely mentioned in this case.



a) False captioning Image

Figure 1.7 False captioning forgery

1.2.8 Forgery Fields

In this section, the fields where the forged digital images are used simultaneously are listed.

1) Counterfeiting: In currency duplicating, license duplicating, identification duplicating etc. the image forging are used.
2) Evidence tampering: In back dating, insurance fraud, introducing psychological bias etc. forged images is used for altering the evidence.
3) Antique faking: In E-commerce, the online products are the showcase with fake images attracting the users.
4) Political propaganda: In politics, the forged images of the ministers are used to spoil their name, and take along shame on them.
5) Yellow journalism: In journalism, the forged images are used to present non-legitimate news to sell more newspapers, magazines etc.
6) Scientific research: In scientific community, the results and observations of the research works are forged.
7) Entertainment: In entertainment filed, the forging is more concurrent. This is performed to increase the target rating point. Moreover, in films, shows etc. the forged images are utilized.
8) Urban myths: The forged image in creating ghosts, Unidentified Flying Object etc.

1.3 Image Authenticity

Image authenticity is the verification process to identify whether the image is forged or not Shi, Yun Q., et al (2007). “Keep it real” is the slogan concerned with the image authenticity. The truth behind the authenticity is substantial, in some cases the forged images are prepared for some showbiz tenacity but it may intentionally affect the lives of another in one form or another. Such effect mounts the image authenticity as a decisive step. But in present world, the image authenticity is difficult to realize because of the different types of the forgeries. Also,the tampered image doesn’t leave any visual clue after underlying manipulation process. This calls for the reliable forgery detection technique to authenticate whether the image is fake or original.

1.4 Image Forgery Detection

The need for the image forgery detection is increasing because of the threatening situation offered by the sophisticated image modification tools which diminish the credibility and authenticity of the original image Farid, H.,(2009). This worse situation entails image forgery detection as an active area of research. Despite a hot topic in research community, only few works have been performed in image forgery detection but the need for more erudite detection algorithm is increasing. In fact, almost all of the image forgery detection techniques aim at detecting the composite operation (forgery type) used to manipulate the image. At present different type of detection algorithms exist, but the general structure appears same with changes in concepts for detection the fake images. The general structure of the image forgery detection is presented below,

General structure of image forgery detection

The fabric of the image forgery detection consists of four processing stages. They are

(1) Image pre-processing
(2) Feature extraction
(3) Classifier selection
(4) Classification

Figure 1.8 depicts the general structure of the image forgery detection. Primarily, image pre-processing is performed over the image subjected for the authentication. Subsequently, the feature extraction is performed over the pre-processed images. The feature extraction may require different segmentation mythologies for the separation of the tampered objects. Afterwards, the image is classified as fake or original one based on the credibility. In classifier phase, primarily, the appropriate classifier is selected. The classifier selected must be apt

for the extracted features. The classifier selection is ambiguous, since the image contains different inconsistencies. Afterward, the extracted features are given to the selected feature and classification process is performed authenticating the image.

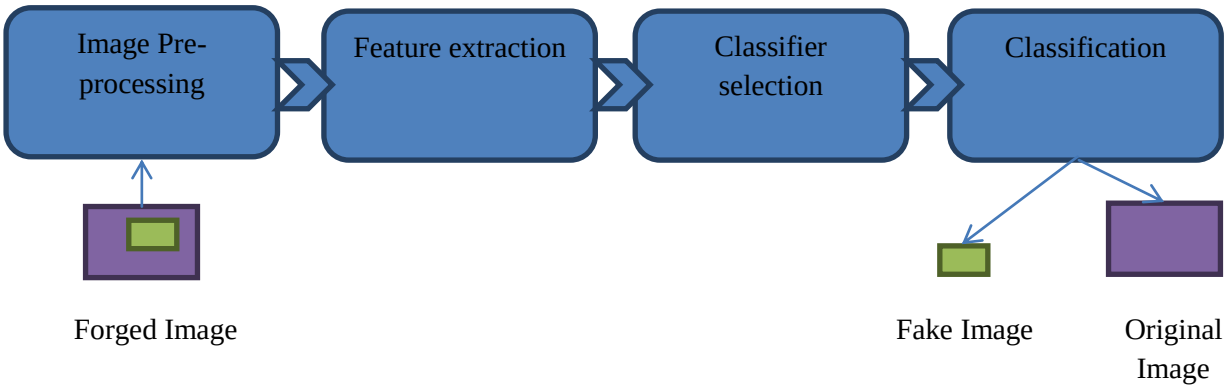


Figure.1.8 General Structure of image forgery detection

The image forgery detection is classified into two approaches centred on the prior knowledge requirement for the forgery detection. They are

1) Active approaches based forgery detection
2) passive approaches based forgery detection

1.4.1 Active Approaches

Active forgery detection is the traditional method used for the detection of the image manipulation. Dynamic approaches verifies the authenticity of the image by means of hiding schemes. Watermarks or digital signatures are the data hidden in the image at the time of creation Al-Hammadi M.,(2012). At the date of the recovery in the receiving end, the secret data or signatures are recovered and verified with the stored data for verification process. The original image may or may not be required at the received end during the check. The data recovery verification process in presence of original image is called non-oblivious data approaches and the data recovery verification process in absence of the original image is called oblivious data hiding method respectively. The authentication

methodology for active approaches require specialized implementation tools i.e., both hardware and software for the creation of the water mark or digital signature as well as the saving. The detailed description about the active approaches is presented below;

(i) Digital Watermarking:

In digital marking based active approaches, a paticular digest is inserted into the original image at the time of capturing. The authenticity of the image can be verified at any instance by extracting the digest. When the digest differ from the original one, the image is considered as a manipulated image. Judith, A et al (2007).

(ii) Digital Signature:

In digital signature based active approaches, the unique properties of the captured image are extracted as signature from the image at the capturing end. In authentication process, the properties of the pictures are regenerated and matched. While matching, if the signature is found varied, the image is considered as tampered image BarnaliSarma, Gypsy Nandi, (2014).

Advantages:

The significant benefit of the active forgery detection approaches is low computational cost. Furthermore, hiding based detection method need simplified knowledge for verification process.

Disadvantages:

The shortcoming of the active forgery detection approaches ascends with the requirement of prior knowledge of original image. The experience dependence epitomizes the need for the human intervention. Moreover, creating digital images with digital watermarks is unfeasible to achieve. Besides, in occasion of hiding signature the need for the extra bandwidth to transmit the name appears to be a disadvantage Kaur, H. and Kaur, K., (2015).

1.4.2 Passive Approaches

Passive forgery detection criteria are exact contradictory of the active approaches. Passive approaches authenticate the tampering of the image without any prior knowledge of the original image or its features. In order to verify the genuineness of the image, the statistics and content of the available image are utilized in the passive approaches. The verification process is performed based on the information of the picture itself without using any additional information. Since the passive approaches authenticate the forged image based on the available knowledge, it is also called as blind approach. The brief introduction about the passive approaches based forgery detection techniques is available in B. Mahdian and S. Saic.,(2009), B. Mahdian and S. Saic.A(2010), H. Sencar and N. Memon.,(2009). The detection techniques in the passive approaches are categorized into two types.

1) **Source device identification**: The source device identification technique is used to identify the origin of the forged image. For example, if an image of some crime scene is found to be manipulated, the source i.e. camera used for capturing the image seems to be the evidence of the corresponding crime and if the camera of origin is identified, the culprit can be easily identified. The source device identification approaches uses the traces that are left during the image acquisition and the storage phase. The various number of camera models are available in the digital photography, in perspective of identification the camera is distinguished based on the camera finger print.

2) **Forgery detection**: This technique deals with the verification approaches of the image itself. It is either forgery type dependent or independent. The forgery-type dependent detection techniques are designed for specific types of forgeries, such as copy-move or image splicing, while the independent techniques are designed to detect forgeries regardless of the type of the forgery. The decisive steps in the

forgery detection are i) Authenticity decision, ii) Forging operation identification iii) Manipulation Explanation and iv) Suspicious area localization. Figure 1.8 specifies the decisive steps involved in the forgery detection.

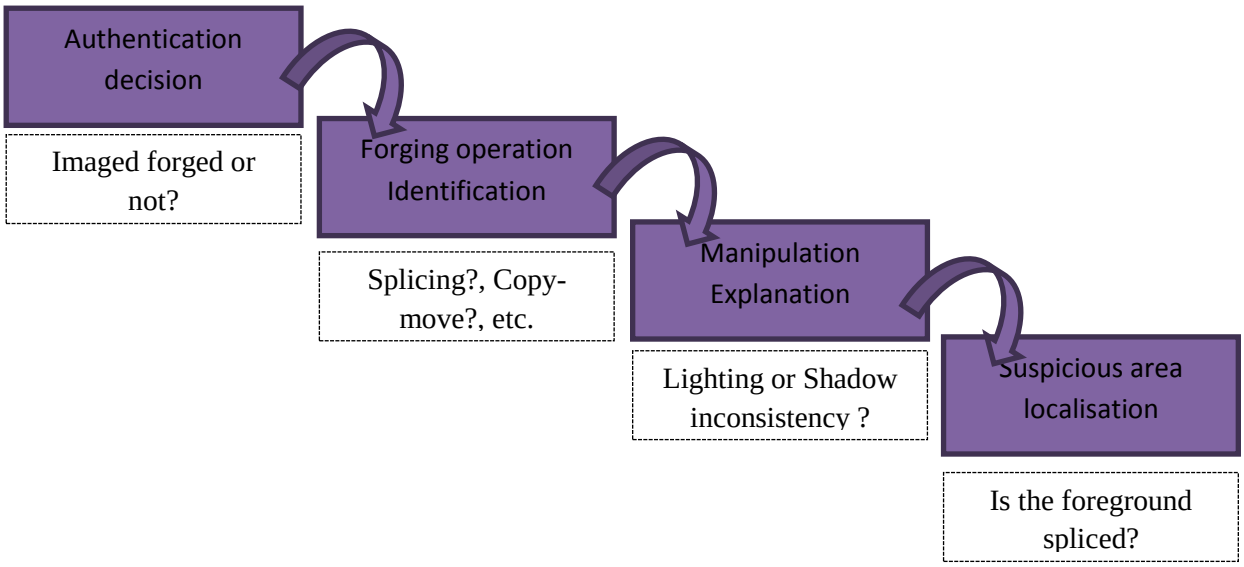


Figure.1.9 Decisive steps in forgery detection

In figure 1.9, under each decisive steps, some questions are mentioned which are answered by the corresponding steps. Primarily, the decision regarding the image manipulation is done in authentication decision step i.e. whether the particular image is forged or not. Consequently, the forging operation in the image is identified in forging operation identification step i.e. whether the image is forged with splice forgery or enhancing forgery etc. Intend of the manipulation is explained in manipulation explanation step i.e. manipulation of image is identified based on the lighting inconsistency present in the image or is it because of the shadow reflection inconsistency etc. present in the image. Finally, the suspicious area in the image is localised from the image by suspicious area localisation step separating original and the fake image i.e. stock photo.

In recent years, the research interest on the passive digital image forgery detection is increasing. The passive image forging detection technique is classified

into different types based on the level of obligation. Figure 1.10 depicts the level based categorization of the passive image forgery detection techniques.

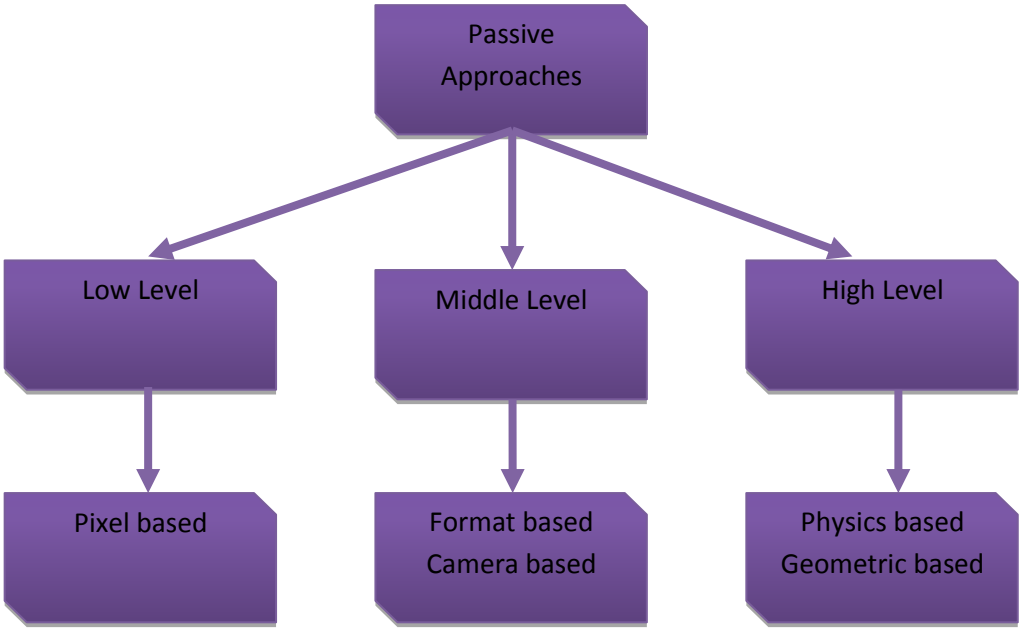


Figure 1.10 Types of Passive Image Forgery Detection

Low Level: In Low level, the passive forgery detection techniques that use characteristics of the digital image pixels for the detection purpose is enumerated. Action over DCT coefficients of the images also comes under the low level methods. Pixel based detection technique is the low level passive image forgery detection technique. In low level methods, no additional sematic information is inserted by the forgers into tampered images.

Middle level: In middle level, the forgery detection methods which aim to detect the tampering operation performed to manipulate the image with small semantic information change over are enumerated. Format based detection techniques, camera and camera based detection methods are the middle level passive image forgery detection technologies.

High level: In high level, methods which have the ability to detect the forgery in images which are completely varying from the original image are employed. The

physic based detection technique and geometric based detection techniques comes under the high level passive image forgery detection technologies.

The most common types of the forgery detection techniques are

(i) Pixel based techniques

(ii) Format based techniques

(iii) Camera based techniques

(iv) Physics based techniques

(v) Geometric based techniques

(i) Pixel based techniques:

Pixel based techniques identify the forgery in the original image by analysing the pixels constituting the image. The processing steps involved in the pixel based techniques are, primarily, the image pixels of the test images are evaluated and the image pixel collection having random intensity signifies the fact that the images are forged. Pixel inter correlation occur in forged images either directly or indirectly because of the tampering operation either with small semantic information change or with larger semantic information change. In initial works of pixel based techniques, instead of pixel, the block analysis is performed to detect the ambiguousness. In block based methods, the image subjected to forgery authentication is divided into blocks and individual blocks are matched with each other. The image block which differs from others resembles the localized area of tampering. Principal Component Analysis (PCA) J. Fridrich (2003) and Discrete Cosine Transform (DCT) A. Popescu and H. Farid., (2004) are the two most prominent techniques used for searching matching blocks in the image. Some of the pixel based detection techniques are deliberated in S. Bayram, et al (2006), H. Farid and S. Lyu (2003), S. Lyu and H. Farid (2005), T.-T. Ng and S.-F. Chang,(2005).

(ii) Format based techniques:

Format based techniques detect the forgery in the images based on the changes in the image format. The leverage of the tampering operation in image

format is infeasible. The steps involved in the format based techniques are, primarily, the images are divided into DCT blocks and quantized which results in coefficients. The quantization coefficients are determined from the quantization table. This is one of the compression techniques. This raises certain artifacts in the image which can be used for the forgery detection. The artifacts occurrence is because of the presence of horizontal and vertical edges between the blocks due to independent transformation and quantization of each block from other blocks. The quality of the image and its size is determined by the quantization table, tends to differ between camera manufacturers which can exploited to perform a forensic analysis on the image to determine its source camera H. Farid (2008), M. Liu et al (2010).In earlier format based works J. He et al (2006), F. Huang et al (2010), J. Luk´aˇs and J. Fridrich (2003). difficult case of quantization matrices for the compression techniques are presented for the forgery detection. In such cases, only the bulky matrices are analysed to detect the artifacts and to provide evidence of manipulation. Image tampering with aberrations also results in the artifacts which are detected by the format based methods W. Luo et al (2007), S. Ye et al (2007), T. Bianchi and A. Piva (2011).

(iii) Camera based techniques:

Camera based techniques detect anomalies in the image by exploiting the artifacts introduced by the camera lens, imaging sensor, sensor noise etc. Inconsistencies in these artifacts can be used as evidence of tampering S. Bayram(2006). The processing steps involved in the camera based techniques are, primarily, the camera is used to capture the image. Some artifacts are present associated with the captured image because of the aberration in the camera lens, imaging sensor, etc. These artifacts manifest the presence of image forgery because of varying characteristic of the camera. In earlier works of camera based techniques, artifacts due to camera lens aberration are most common M. Johnson and H. Farid(2006), T. Van Lanh et al(2007), I. Yerushalmy and H. Hel-Or(2011). The reason for artifacts duet to camera lens aberration is presence of dust specks on the

lens. In perspective of the imaging sensor based artifacts, in most of the digital cameras single CCD or CMOS sensor is used to capture the colour image to keep the manufacturing cost low. In sensor elements, the colour is recorded by the process of demosaicking adopting bilinear, bicubic, or adaptive algorithms. In some cases, the correlation introduced by the colour channels also introduces artifacts in the images S. Bayram et al(2006), H. Cao and A. C. Kot(2011), A. Popescu and H. Farid(2005).

(iv) Physics based techniques:

Physical based techniques detect anomalies in the images utilizing the interaction between physical objects, light, and the camera M. Johnson and H. Farid(2005). In a forged image, inconsistency which can be easily identified is shadow which is concerned with the type of camera used for capturing the image, light and the physical objects at the capture site. The difference in the lighting in the image resembles the possibility for the tampering operation. In the physic based techniques, the detection is performed on three bases.

i) **Lighting**: In lighting based detection, the difference in the lighting of the images is used as evidence for the forgery detection.

ii) **Lighting direction**: The lighting direction of the various points in the image is also used for the detection

iii) **Shadows**: The shadows inconsistency due to the tampering can also be used for the detection.

Using these three, forgeries are exposed by the physics based techniques. The processing steps involved in the physics based techniques are, primarily, the features of the images concerned with lighting, lighting direction or reflection is extracted utilizing different segmentation techniques. Conversely, the constraints of the original image are extracted and matched for detecting the forgery. Human intervention is necessary for physics based detection techniques E. Kee and H. Farid(2010).

(v) Geometric based techniques:

Geometric based techniques detect the anomalies present in the image by exploiting the inconsistencies in the reflection of objects, imaging plane J. Beis and D. Lowe (1997) etc. Geometry difference between the authentic and tampered image is emphasized by the geometric based techniques. The geometric indifference ascends in the tampered image because the real objects in the images are non-uniform in nature but the forger objects are relatively smoothed surfaces with unsuitable lighting assumptions. Such condition leads to geometric differences. Various techniques for geometric based technique are presented in recent years T.-T. Ng et al (2005), S. Bravo-Solorio and A. Nandi(2009). The processing steps involved in the geometric based techniques are, primarily, the features of the images are extracted centred on reflection of the objects, and then difference between the geometric expressions of the image reflection is used for the forgery detection. The detailed description is provided in following sections.

1.5 Forgery shadow detection:

Shadows are essential part of an image. The shadow based detection is the most convenient forgery detection procedure W. Zhang et al (2009), Q. Liu(2011). This is because, when a forger tampers the image, the only concentration is centred on manipulating the objects present in the image which results in shadow inconsistencies of the image. By analysing the shadow properties of the image, the tampering operation performed for the manipulation can be recognised. The shadow in the image is formed by the unruffled action of the light source and the occluding object present at the time of capture. The geometric appearance of the shadow depends on the shape of the occluding object and the receiving plane, conversely the arrangement is similar to that of the object. When the light from the lighting

source is obstructed by the occluding object with respect to the receiving plane, shadow is formed.

The shadow region is classified into two; umbra (dark) and penumbra (less dark). The dark region in shadow is because of complete riddance of occluding object from the light source, whereas in the less dark region the light source is partially hidden from the occluding object Bin Yang et al(2015). Based on photometric properties of shadows in which the shadow does not obviously change the surface texture of object and the fact that both the position and strength of the light source can be estimated from shadows assist in forgery detection. In perspective of the shadow based detection, the shadow vanishing point of the object in the image is calculated and matched with the shadow vanishing point of the image, the mismatch in shadow vanishing point epitomize the image manipulation. For any type of forgery, shadows are the necessary part of an object to maintain the integrity. The consistency variation ascends with tampering in shadow which signifies the presence of forged images. W. Zhang et al(2009), Q. Liu et al(2011). The feature selection construing in the vanishing point estimation always seems knotty in the shadow based forgery detection.

1.6 Forgery reflection detection

Forgery reflection based detection is another crucial forgery detection methodology O. James and H. Farid(2012). This type of detection method utilizes the inconsistencies of the image reflection for the forgery detection. Reflection occurs in an image, when the light from the source bounces off a surface and penetrate through the aperture of the plane mirror. This appeal can be conceptualized by the following example, when an object is placed in front of the mirror, light rays from the objects pass on through the mirror in various directions, and the incident rays are reflected back by the mirror. The reflection of the image is generated in the place where all the reflected rays from the mirror intersect. In

perspective of the reflection based forgery detection, reflection vanishing point of the corresponding reflection of the image is calculated initially. The reflection of the original image and their corresponding reflection must converge in a common RVP to be authentic. The inconsistency in the RVP signifies the presence of the manipulation in the image. The limitations in the reflection based forgery detection algorithms are concerned with the accurate selection of the features from the images, even a small uncertainty in feature selection results in faulty convergence of the RVP. Moreover, the reflection based detection methodology is unfeasible in image containing multiple features without appropriate feature extractor.

1.7 Need for the study

- Geometric inconsistencies due to shadow and reflection can be detected using shadow based detection or reflection based detection technique. This research focuses on developing shadow and reflection individually and paralleled scheme.
- This research will not propose new method for extraction of feature points or segmentation, but will optimally select the design concept as per the need.
- For evaluation, the comparison will be made regarding the detection accuracy and MSE for parallelized detection scheme, periodicity map for shadow and reflection based scheme.

1.8 Problem statement

Passive approaches based detection technique are applied for the image forgery detection since it is more advantageous than the active approaches which utilize prior knowledge about the image for the authentication. The passive approaches acceptance with computational risk is considered tolerable because of its capability to detect the fake images forged with any image forgery. However, the

forgery image with shadow and reflection inconsistencies always appears to be a problem. The major challenges in this research are

Challenge 1: To detect the image forgery with shadow inconsistencies. The first challenge taken here is shadow detection based forgery detection. In shadow detection, the lighting consistence always appears to be a trouble.

Challenge 2: To detect the image forgery with reflection inconsistencies. The second challenge is the reflection detection based forgery detection. The reflection detection should be done in a way to separate the lineated reflection from the original images.

Challenge 3: To combinely detect the shadow and reflection inconsistencies in the forged images. The third challenge is forgery detection approaches with combined shadow and reflection inconsistency detection.

Challenge 4: To select the segmentation techniques for shadow and reflection detection. The fourth challenge is concerned with the segmentation technique required for extracting the useful constraints of the shadow as well as the reflection from the forged images for the classification. The segmentation technique with restored facility is always an pertinent choice.

Challenge 5: To design passive detection approaches with ability to detect any image forgery. This challenge is most crucial one. This is because the design of the forgery detection system with capability to detect any image forgery is always a paragon.

Challenge 6: To increase the detection accuracy. The sixth challenge is concerned with the detection accuracy of the image authentication.

Challenge 7: To design a new classifier with increased detection accuracy. The new classifier with changing ability to decrease the error in classification is obligatory.

The ultimate intend of this research is to find answer for this challenges in a user friendly way to increase the trust among the currently used digital images.

1.9 Objective of the study

The main objective of this research is to develop new shadow based detection technique, reflection based detection technique, and a parallelized detection technique with proper solution for the research questions and challenges. The objective of this research are given below,

Objective 1: The first objective of this research is to develop a geometric technique to identify the shadow vanishing point and reflection point in the image with fraudulent shadowing and reflection. By proper representation, the vanishing points can be inserted into the image for the analysis.

Objective 2: The second objective of this research is to select some segmentation methods for separating the shadow and segmented region and also feature extraction technique to extract the feature points from the geometric inconsistencies.

Objective 3: The third objective of this research is to develop a new detection scheme with ability to parallel detect the shadow and reflection fraudulent image.

Objective 4: The fourth objective is to select efficient technique for segmentation of shadow and reflection region combinely from the image assisting in parallel detection.

Objective 5: The fifth research objective is extraction of proper features i.e. strength enabled feature and texture enabled feature for authentication.

Objective 6: The final objective is to propose a new NN classifier with new learning algorithm for efficient classification of the forged and original image

1.10 Methodology of the study

The image forgery can be easily done by using the powerful image editing tools like paint and Photoshop. These editing tools never leave any evidence of forgery thus, increasing the challenge of the system to detect the presence of the manipulation. The Vanishing point computation method is used to identify the forged region in the shadow based images. The Geometrical representation and collective segmentation analysis is used to identify the forged area present in the reflection based images. In the case of forgery images having both shadow as well as reflection, the forgery can be identified using fuzzy set based segmentation method.

The issue of verifying the authenticity and integrity of the digital image is becoming increasingly important because of the continuous growth of the image communication using which the attackers fakes the visual imagery J. Fridrich,D.Soukal,and J. Lukas, (2003). An image forger manipulates the image vigorously expending different types of forgery (as discussed in section 1.3 of chapter 1). The forgeries appear more frequent now a day in every field where visual imagery is indispensible Ashima Gupta, et al.(2013). On every image capture, the shadow or reflection of the object in the image scene content is inevitable. When an attacker tries to manipulate the special effort in handling the shadow or reflection is obligatory.

The shadow or reflections have to be placed in the forged image with caution without leaving any clue for human perception. In general cases, the shadow/reflection of the object in the image is copied and paste from other image with same object as per the need. In certain cases, the shadow/reflections are manipulated with the existing one. However, the faking procedure of the shadow or reflection results in some geometric inconsistencies. By analysing this inconsistency, the originality of the image can be validated as fake or original one. The shadow or reflection based fraudulent detection is considered so important,

because for every modification made in image for faking, the inconsistency related to shadow or reflection is often overlooked by the forgers. This research is focused on the passive forgery detection approaches such as shadow and reflection based detection approaches.

Before stepping on into the issues that exist in the geometric inconsistency based detection approaches, the overview about the shadow or detection based approaches is necessary. The vast introduction based shadow based detection approaches as well as the reflection based detection approaches is provided in section 1.5 and 1.6 of chapter 1. The process within the shadow/reflection based detection scheme must be first identified and explained. In view points of the shadow based detection scheme, the forged image with shadow inconsistency is initially segmented using segmentation methods.

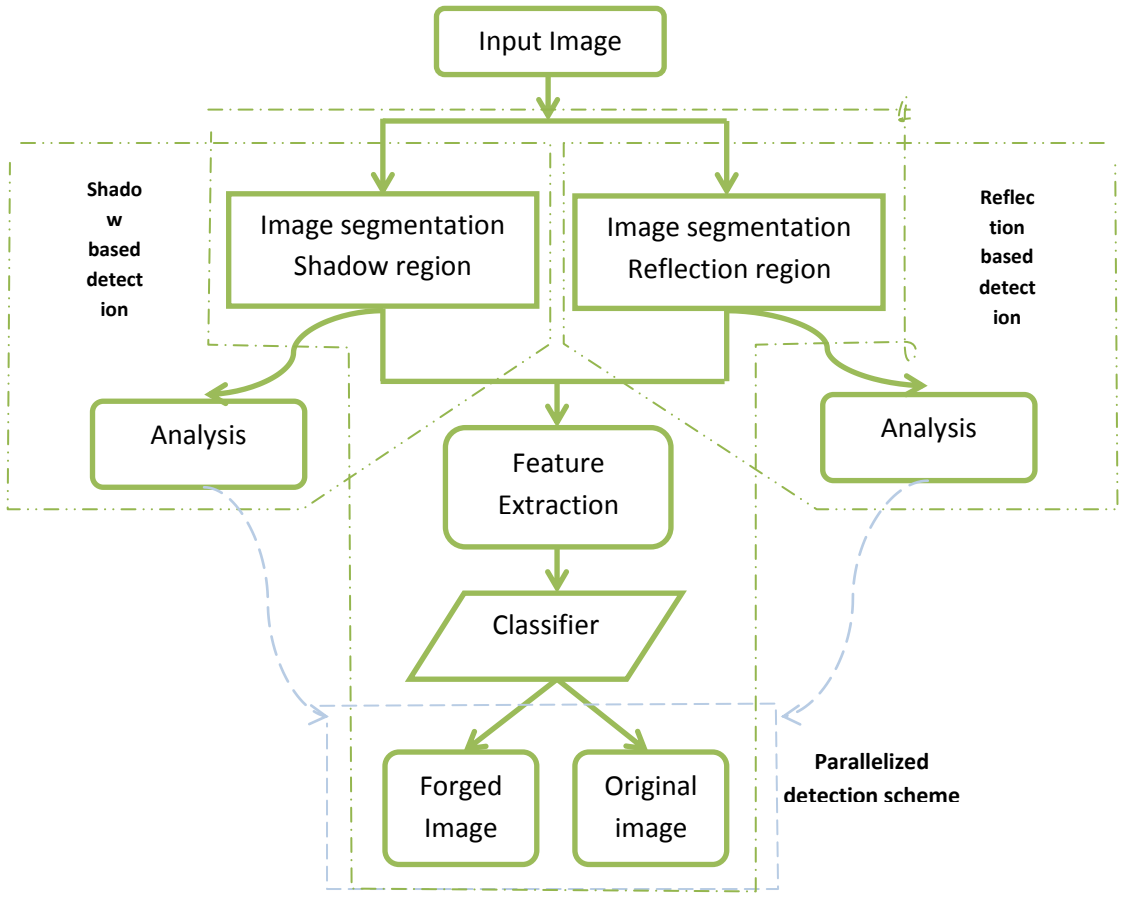


Figure 1.11 Shadow and reflection based detection approaches

The segmentation procedure separates the shadow region from the image. By analysing the shadow point with the original light point of the image, the authenticity can verified. In view point of the reflection based detection scheme, the forged image with reflection inconsistency is primarily segmented using segmentation method. Based on the segmented reflection region, the analysis is performed to discover the forgery. The flow of the shadow and reflection based detection approaches is depicted in figure 1.11. Here the common flow of the shadow as well as reflection based detection approaches is epitomized. Currently, various research works of reflection and shadow based detection scheme is available (Chapter 2). Some of the serious issues in the geometric inconsistency based detection approaches are concerned with the computation time, segmenting algorithm etc. Sevinc Bayram et al.(2009). In real time and near real time application, the computation time of the geometric inconsistency based detection approaches is high and the impact of the segmentation technique for separating the inconsistent shadow or reflection region per the detection rate and false detection rate is also crucial. The solution for such cases is development of the parallelized detection scheme i.e. combinatorial shadow as well as detection scheme. The mere development parallelized scheme can reduce the computation time and segmentation disadvantages. The robustness of the detection algorithm can be improved in the distinctive shadow based detection approaches by proper representation and segmentation concepts likewise in reflection based approaches, the proper segmentation concepts can play its significant role.

In parallelized detection approaches, the proper handling is needed in segmentation of shadow and reflection region, feature extraction, classifier etc. Moreover, the performance and viability of the detection scheme must be compared for duplication matching. This research step forwards to craft new shadow based detection technique, reflection based detection technique and parallelized detection technique. In existing approach forged reflection based images and shadow based

images are individually detected. In proposed approach the forged images are detected individually as well as paralleled. In my research the Computation time is less with high accuracy.

1.11 Limitation of the Study

One of the limitation is the noise present in the different region of the image varies, so that the 100 % accuracy in the image authentication cannot be determined. The another is the shadow and reflection detection of the image authentication is inaccurate due to poor lighting.

1.12 Organization of the thesis

The organization of this thesis is presented in this section. This thesis is organized into nine chapters. Chapter 1 gives a vast introduction about the image forgery, types of image forgery, Scope of the shadow and reflection based detection and approaches for forgery detection is followed by the chapter 2.

Chapter 2 reviews the available relevant literature regarding the forgery detection techniques. The literature begins with the categorisation of the existing works, followed by review of different image forgery types. The literature also highlights the advantages and disadvantages of the existing forgery detection techniques along with segmentation methods and describes the machine learning techniques for the shadow and reflection detection in inconsistent forgery image.

Chapter 3 describes the proposed vanishing point based shadow detection method developed for the image forgery detection. The different image segmentation techniques utilized for segmenting the vanishing points are also detailed. The experimentation results and the analysis of the proposed method are also provided in this section.

Chapter 4 describes the proposed reflection points based detection method developed for the forgery detection in image with reflection inconsistencies. The segmentation methodologies and geometric representation utilized in this method are also discussed. The experimentation results and analysis of the proposed method are also provided in this section.

Chapter 5 presents the detailed description about the proposed consistency feature and fuzzy set based segmentation based image forgery detection. The new ABCLM based neural network classifier developed for classifying the fake and authentic images are deliberated in this section. The authentication results of the proposed method regarding accuracy and MSE are also presented. Chapter 6 presents the research conclusion, and the suggestion for the future studies.

In this chapter, the introduction for the research in the shadow and reflection based technique is presented. The challenges, research questions, research objectives and research scopes are also addressed. The utmost intend of this research is to develop new shadow based detection technique; reflection based detection technique and parallelized detection technique for validating the authenticity of the image. The research goal is to develop detection methods with efficient performance in terms of detection accuracy.