Introduction

1. INTRODUCTION

In modern times, the traditional paper media is being replaced with its digital versions for gaining the advantage of avoiding large storage and preservation requirements, while making information easily available for a larger number of users. Almost all commercial and private organizations are now moving towards 'paperless' office, where common office devices such as digital photocopiers, fax machines, scanners, digital cameras and camcorders are increasingly used to create digital contents. They have advantage that the digital form can be easily created and stored.

In recent years, tremendous growth has been witnessed in the development of modern technologies like Internet, P2P (Pear-to-Pear) and MMS (Multimedia Messaging Services), which make an important evolution towards digital distribution of data via networks. Moreover, several transmission devices and techniques like General Packet Radio Service (GPRS), Multimedia Messaging Services (MMS), Video Clip transmission, High Definition Television (HDTV) and Video Conferencing are being used by more and more people for faster and easy communication.

These digital transmission techniques have introduced flexible, cost-effective communication models that are advantageous for electronic commerce transactions. As a result, digital content appear widely in the Internet and the World Wide Web (WWW) and in storage media such as CD-ROM and DVD. The past few decades have envisaged tremendous increase in the usage of multimedia content, especially, digital images. Several innovative techniques are used both by professionals and common population to create digital images.

Today's computer-enhanced digital doctoring, images have become a fertile ground for forgery. With the ever changing advancements in imaging software like Adobe PhotoShop and CorelDraw, it is now easy to manipulate and edit images without noticeable traces. Thus, easy access facilitates has

introduced information misuse, through unauthorized replication and manipulation of digital data (Surekha *et al.*, 2010; Karen, 2003) allows a pirate (a person or organization) to violate the copyright of real owner. For example, there were reportedly five million registered users at www.worth1000.com in 2004, out of which, 37.1% of users created and published photomontage images with image editing software in the hopes of receiving the most votes for a prize. The high quality of some images made it difficult to determine whether they were original or altered.

This makes confidentiality and integrity as mandatory requirements against unauthorized data duplication, modification and illegal distribution of digital content (Bert and Cave, 2000). This has forced academicians, industrialists and researchers to focus on the development of techniques for the protection of digital images through detection of manipulations or modifications. Image tamper detection is a field that is connected to this issue. It has high relevance with forensics where most often images are used as legal evidences.

In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is important. In medical field physicians and researchers make diagnoses based on imaging which is crucial as one is dealing with human life. E-commerce has drastically increased in recent years due to advancement of information technology and the internet. As per the world internet statistics, from 2000-2005 a growth of 160% has been reported. This is currently a market of approximately 50 million internet users who have made an online retail purchase. This cohort will grow to nearly 100 million internet users by 2008 and will be responsible for nearly 90% of all online retail sales by that time (http://www.internetworldstats.com/stats.htm).

Online marketing is mainly based on multimedia technology with images and video as basic elements of product description. With the increase

of sophisticated and advanced image processing and manipulation software's coming in to markets, even a novice has gained with power to tamper images and counterfeit revising the age old saying "A picture is worth a thousand words" to "A picture unworthy a thousand true words". The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media (http://wiki.media-culture.org.au/index.php/Digital_ Image_Manipulation_Journalistic_ Integrity).

Forensic image authentication or originality testing is the application of image science and domain expertise to discern if a questioned image is an accurate representation of the original data by some defined criteria. Several techniques like watermarking, steganography and tamper detection algorithms are used for this purpose. This research focuses on tamper detection algorithms.

Digital images can be manipulated using various techniques like data removal, replacement, replication, photomontage, or computer-aided media generation. Out of the various techniques, photomontage is gaining more importance. Photomontage is the technique of making a picture by assembling pieces of photographs, often in combination with other types of graphic material. When dealing with the photomontage detection problem, one of the fundamental tasks is the detection of image splicing. Image splicing assumes cut and paste of image regions from one image onto another image. A spliced image can be detected if individual regions within it have different camera signatures. Motivated by this fact, this research work uses the digital camera statistical characteristics to detect sliced image forgery. The concepts behind image tamper detection with focus on sliced image forgery are presented in this chapter.

1.1. DIGITAL FORGERY AND IMAGE TAMPERING

A digital image is a data representing a two dimensional scene and are used in almost all fields of applications. With the availability of state-of-the art economical cameras and easy-to-use image editing software, has opened the world of creativity to modify images, either intentionally or unintentionally.

The hierarchical overview of different forms of digital forgeries is presented in Figure 1.1 with the research interest area highlighted.

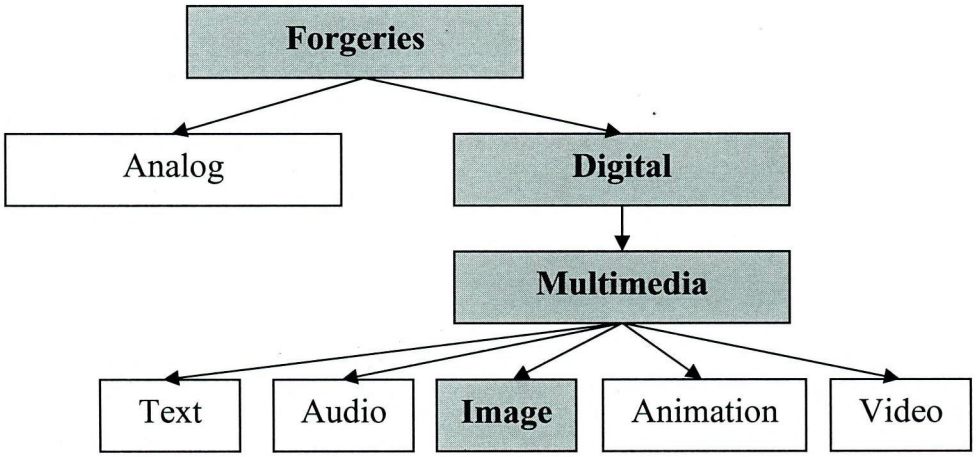


Figure 1.1 : Digital Forgeries

The field of digital forgery had drawn the attention researcher worldwide. The problems being highlighted in this domain are digital forgeries of social impacts, detection techniques, and prevention techniques. The digital forgeries have many perspectives and implications on social, legal, technical, intelligence, investigative mechanisms, security, managerial issues.

Forensics is the art or study of argumentative discourse where science is used to provide facts i.e. applying science to law. It is a technique for the identification, recovery and the reconstruction of evidence. Forensic Science investigators reconstruct/extract evidence that can be applied to criminal cases to provide further leads, or conclude facts. Computer Forensics has adopted a similar investigative procedure but the scientific examination is solely

concerned with the data held on, or retrieved from, digital media. Therefore, Computer Forensics can be defined as the preservation, identification, extraction, documentation and interpretation of computer data (Barrett, 2004).

The forensics techniques are primarily divided in three categories (Sencar and Memon, 2007):

- **Image forgery detection** : This is used to prove that a a-posteriori manipulation has been applied to an image, e.g., moving or replacing an object within an image. Different tools, such as binary similarity measures, wavelet coefficient statistics, quality metrics, phase characteristic of the bicoherence spectrum, resampling, color filter array interpolation, and geometric optics can be used to this aim.
- **Discrimination between synthetic and real images**
- **Image source identification** : Here, all methods are based on the assumption that digital pictures taken by the same device are overlaid by a specific pattern, that is a unique and intrinsic fingerprint of the acquisition device. Each manufacturer selects specific hardware components for a given device model, thus different patterns can be present in the image, depending on the brand and on the model. These intrinsic characteristics allow linking images to a specific device for forensic purposes. Many techniques have been proposed in the literature to describe this unique pattern, each one analyzing different processing steps of the digital camera pipeline (i.e. demosaiking, CFA interpolation, lens radial distortion). The most promising approach belonging to this class of forensics techniques is based on the analysis of sensor imperfections. Two types of noise have been considered in forensics analysis. The first type is introduced by array defects and includes hot pixels, dead pixels, pixel traps and cluster defects. The major drawback of these methods is that defect pixels are not very reliable since many cameras include in their hardware post-processing operations able to compensate such a noise. The second type of noise is called Patter Noise and indicates "any spatial pattern that does not change

significantly from image to image". This reference pattern is known given the camera model that took the photo or is obtained by averaging the noise residuals of a set of available images, all taken from a specific camera.

This research focuses on the third type. The general procedure used by the forensic personals is described as follows. When a photograph is used as evidence in legal cases and its authenticity is in question, the forensic department first requests the photographers to turn in the camera using which the photograph was taken. Then various methods are used to extract features of cameras and image to identify manipulations or modifications made. This research work proposes algorithm that can aid in these situations, by utilizing the statistical features of a camera to identify tampering in images.

1.2. CONTENT ALTERATION OPERATIONS

The digital information revolution and issues concerned with multimedia security have also generated several approaches to tampering detection. Generally, content altering operations can be classified into the following groups.

- **Removing**

This group is defined by operations that remove some parts from the multimedia content. The operations, including cutting and wiping, are often applied in either a spatial or temporal domain. Removing a moving car from a picture, cutting a segment from a voice sequence and deleting a person from a frame in video sequence represent examples of this practice. Generally, this operation is combined with other operations like filtering and noise removing, to obtain the desired quality or effect on the content.

- **Replacement**

This group includes operations that replace some parts of multimedia content with parts borrowed from other content. Some examples are : replacing a person's face in a photo with one from another photo, replacing a

segment from an audio sequence with one from another sequence and replacing a moving care in a video sequence with another. Generally, these replacements are achieved by combing several operations, such as wiping, pasting and smoothing.

- **Replication**

This group includes operations that increase the number of objects in the content by copying and pasting them from one location to another. For example, copying an image of an airplane and pasting it into other locations in the picture increases the number of airplanes. Generally, replication is achieved by combing several operations such as, copying, pasting and smoothing.

- **Photomontage**

This group includes operations that combine several pictures, producing new one of high quality that is typically a collage. Generally, photomontage is achieved by performing several additional operations such as cutting, splicing, filtering, pasting and smoothing. As this is the primary topic in this research, it is explained separately in the following section.

- **Computer generated media**

This group includes media content generated by computers, for example, computer graphs and computer aided drawings. Only the natural scene is simulated so the resulting media content is different from the natural one. Cartoonization is one type of computer aided drawing technique that converts natural digital images into animated digital media. Simple examples of manipulated images are shown in Figure 1.2.

Figure 1.2 : Examples of Image Tampering
Source : http://www.famouspictures.org/mag/index.php

1.3. PHOTOMONTAGE

Photo manipulation is the application of image editing techniques to photographs in order to create an illusion or deception through digital means (Michael, 2009). Manipulation is defined as the modification of image features by direct alteration of image content at the pixel/voxel level. Common manipulation techniques amenable to analysis involve primarily alteration and compositing. Alteration is the changing of image features through the use of artistic means.

Photomontage, a general operation used in image forgery, is essentially a collage containing several existing images. Photomontage is a paste-up produced by sticking together photographic images, possibly followed by post-processing (e.g. edge softening and adding noise). Photomontage, with a root as old as the history of camera, is now a looming threat in the field of image authenticity.

Lack of internal consistency, such as inconsistencies in object perspective, in an image is sometimes a telltale sign of photomontage (Mitchell, 1994). However, unless the inconsistencies are obvious, this technique can be subjective. Furthermore, forgers can always take heed of any possible internal inconsistencies.

In today's scenario, image authenticity can no longer be taken for granted especially when it comes to legal photographic evidence and electronic financial documents. Therefore, a reliable and objective way to examine image authenticity is the immediate need. Distinguishing digital images from their photomontage versions involves establishing the integrity of digital images.

At present, there are mainly three kinds of technologies used to identify photomontage forgeries. They are, digital signature technology, digital watermarking and blind identification technology for digital images.

The first two identification means require the image to be pre-processed by its provider, such as extracting the summary or inserting a watermark, etc. And in order to identify the image authenticity, the person conducting identification must know its original summary or watermark, which limits the scope of application of the image identification technology. However, blind identification technology for digital images is one of the new and effective means used of detecting image tampering, which identifies the authenticity of image content relying on neither pre-signature extraction nor pre-embedded information.

Similarly, methods for photomontage detection can be classified into two categories, namely, manipulation-specific methods and classification-based methods. In the first category, manipulation-specific methods are developed with the aim of detecting a particular type of tampering operation such as compression, filtering, gamma correction, and re-sampling. Although these methods work well in detecting a particular type of tampering operation, it would require an exhaustive search over all the possible kinds of operations to establish the integrity of a digital image. In the second category, classifier-based approaches, that utilize features such as image quality or features, are proposed. These techniques provide a framework for universal image analysis independent of the nature of tampering.

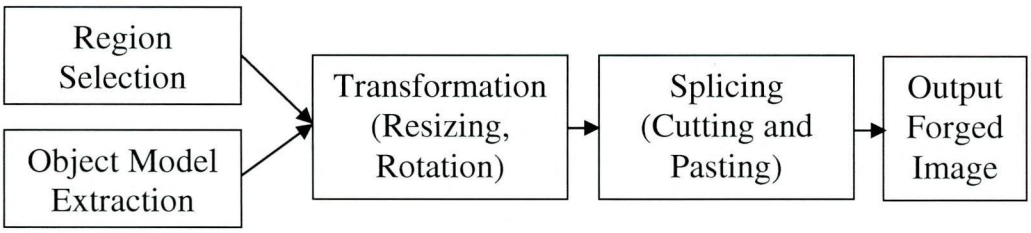
This work proposes blind identification techniques that extract features of digital images to discriminate direct camera outputs from their tampered versions. The basic idea behind this approach is that image manipulations, such as tampering, change the image statistics in specific ways and such changes can be utilized to perform analysis for image manipulation detection.

1.4. IMAGE SPLICING

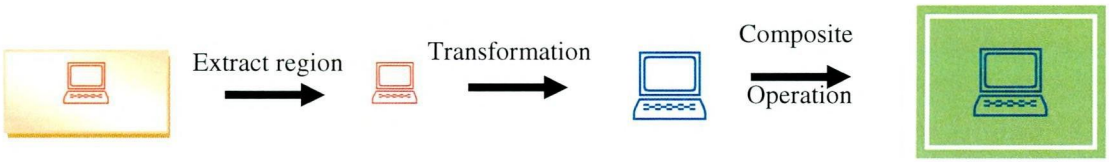
Image splicing is the most fundamental and essential technique used in photomontage. Image splicing is defined as a cut-and-paste of image regions

from one image onto the same or another image without post-processing. Image splicing is the basic operation for creating a digital photomontage, i.e., a paste-up of digital photographic regions.

The basic steps involved in the process of creating a 2D composite spliced image is shown in Figure 1.3a with an illustrative example shown in Figure 1.3b. Although post-processing is often applied to blend the spliced object better to the image background and remove the artifacts from the rough region selection, a spliced image without post-processing can be very realistic for non-experts.



(a) Process Flow for Creating Image Forgery



(b) Illustrative Example

Figure 1.3 : Spliced Forged Image Creation Process Flow with Example

Although this work considers only image splicing, there are specific works in passive-blind image forensics for detecting certain post-processing operations of an image as a tell-tale sign of image compositing. Some examples are given in Figure 1.4.

Image splice image forgery recently has been proved to successfully detect using the camera statistical properties. As the proposed method uses the properties of cameras during forgery detection, the following section is dedicated to a simple explanation on the basic of digital cameras and image pipelining.

Figure 1.4 : Example Photomontage Images

1.5. IMAGE PIPELINING IN DIGITAL CAMERAS

Fueled by the demands of multimedia applications, digital still and video cameras are rapidly becoming widespread. As image acquisition devices, digital cameras are not only replacing traditional film and analog cameras for image captures, they are also enabling many new applications such as PC cameras, digital cameras integrated into cell phones and PDAs, toys, biometrics, and camera networks. Figure 1.5 is a block diagram of a typical digital camera system.

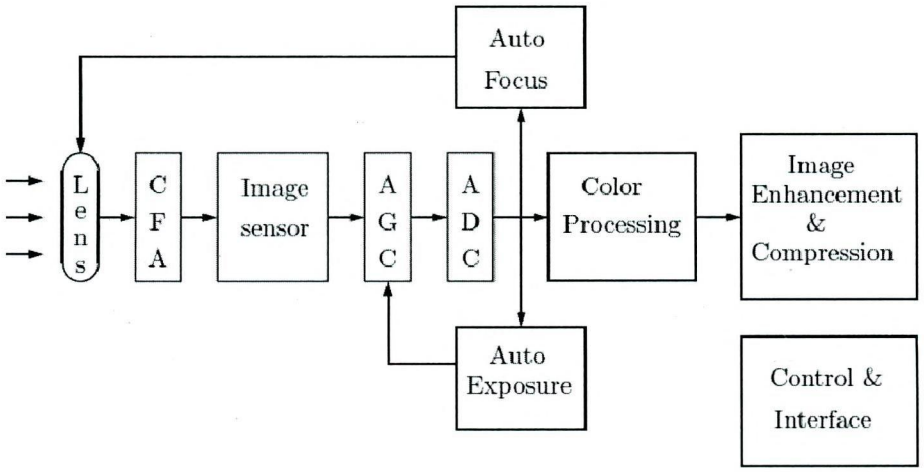


Figure 1.5: A Typical Digital Camera System

In the above figure, a scene is focused by a lens through a color filter array onto an image sensor which converts light into electronic signals. The electronic output then goes through analog signal processing such as correlated double sampling (CDS), automatic gain control (AGC), analog-to-digital conversion (ADC) and a significant amount of digital processing for color, image enhancement and compression.

The image sensor plays a pivotal role in the final image quality. Most digital cameras today use charge-coupled device (CCD) image sensors. In these types of devices, the electric charge collected by the photodetector array during exposure time is serially shifted out of the sensor chip, thus resulting in slow readout speed. Digital cameras are capable of capturing an optical scene and converting it directly into a digital format. In addition, all the traditional imaging pipeline functions, such as color processing, image enhancement and image compression, can also be integrated into the camera. This high level of integration enables quick capture, processing and exchange of images. Modern technologies also allow digital cameras to be made with small size, light weight, low power and low cost.Basic imaging pipeline structure is shown in Figure 1.6.

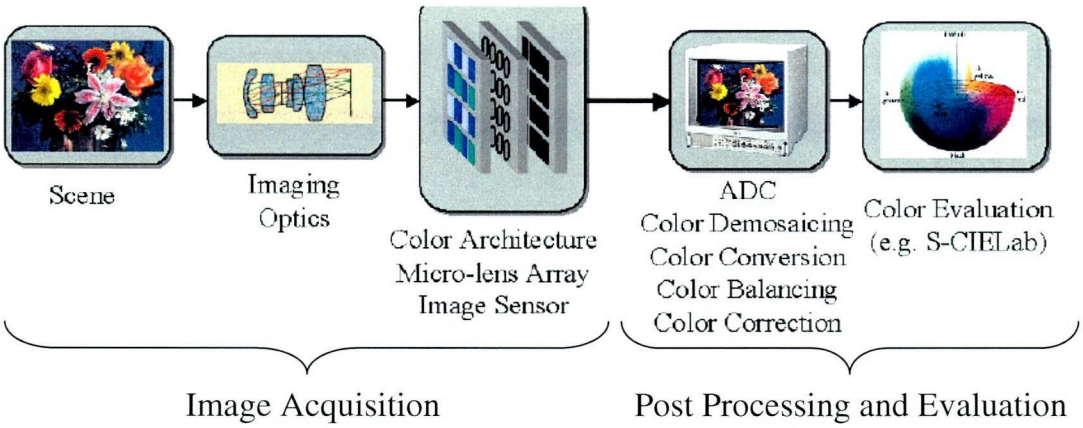


Figure 1.6: Digital Still Camera System Imaging Pipeline

The front-end of the optical pipeline is formed by the scene and is in fact not part of the digital camera system. However, it is very important to have an accurate yet tractable model for the scene that is going to be imaged by the digital camera.

First, the natural light passing through the optic system is "captured" by a sensor (CCD etc.). Generally, only a single CCD detector is used at every pixel in a consumer digital camera. Moreover, the surface of the detector is partitioned with different color filters which are called Color Filter Array (CFA). Then the missing pixels in each color planes are filled in by a CFA interpolation. Finally, operations such as demosaicing, enhancement and gamma correction are carried out in the camera. Usually, after imaging process, the digital image will be converted to a user-defined format, such as RAW, TIFF and JPEG, and stored in the memory.

1.6. SINGLE CLASS CLASSIFIERS (SCC)

Single-Class Classification (SCC) seeks to distinguish one class of data from the universal set of multiple classes, e.g., distinguishing apples from fruits, identifying "waterfall" pictures from image databases or classifying personal homepages from the Web. Since it is not natural to collect the "non-interesting" objects to train the concept of the "interesting" objects, SCC problems are prevalent in real world where positive and unlabeled data are

widely available but negative data are hard or expensive to acquire (Yu *et al.* 2002; Letouzey *et al.*, 2000). For example, in text or Web page classification like personal homepage classification, collecting negative training data (a sample of "non-homepages") is delicate and arduous because manually collected negative data could be easily biased because of a person's unintentional prejudice, which could be detrimental to classification accuracy.

The One Class Classification (OCC) problem is different from the conventional binary/multi-class classification problem in the sense that in OCC, the negative class is either not present or not properly sampled. The problem of classifying positive (or target) cases in the absence of appropriately-characterized negative cases (or outliers) has gained increasing attention in recent years. Researchers have addressed the task of OCC by using different methodologies in a variety of application domains.

The importance of one-class classification can be justified using the following examples. One-class classification can be relevant in detecting machine faults, for instance. A classifier should detect when the machine is showing abnormal/faulty behaviour. Measurements on the normal operation of the machine (positive class training data) are easy to obtain. On the other hand, most faults will not have occurred so one will have little or no training data for the negative class. As another example, a traditional binary classifier for text or web pages requires arduous pre-processing to collect negative training examples. For example, in order to construct a homepage classifier, collecting sample of homepages (positive training examples) is relatively easy, however collecting samples of nonhomepages (negative training examples) is very challenging because it may not represent the negative concept uniformly and may involve human bias.

The one class classifier can be applied in different problems. It can be used for:

- Novelty detection (for machine condition monitoring where faults should be detected),
- Outlier detection (for more confident classification as in the example above),
- Badly balanced data (classification in medical data with poorly sampled classes),
- Data set comparison (to avoid the training classifiers again for comparable data).

This research uses the single class classifiers to detect tampers in a digital image using their camera statistical properties.

1.7. MOTIVATION AND OBJECTIVES

Digital imaging has matured to become the dominant technology for creating, processing and storing pictorial memory and evidence. Though this technology brings many advantages, as mentioned previously, can be used as a misleading tool for hiding facts and evidences. This is because, today, digital images can be manipulated in such perfection that forgery cannot be detected visually.

The security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. These techniques can be divided into two major groups:

- Intrusive and
- Non-intrusive

In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and authenticity is established by verifying if the true signature matches the retrieved signature from the test image (Yeung, 1998; Rey and Dugelay, 2002; Zhang *et al.*, 2008). This approach is limited due to the inability of many digital cameras and video

recorders available in the market to embed extrinsic fingerprints (Farid, 2009).

The limitations of intrusive techniques have motivated the need for non-intrusive (blind) techniques (Mahdian and Saic, 2008; Farid, 2009; Mahdian and Saic, 2009; Lin *et al.*, 2009) to validate the authenticity of digital images. These techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. Verifying the integrity of digital images and detecting the traces of tampering without using any protecting pre-extracted or pre-embedded information have become an important and hot research field of image processing.

There are many challenges in blind techniques, for instance, reducing false positive rates (i.e., an authentic image being detected as a forged image), making the system fully automated, localizing the forgery, detecting forgery of any type of image format (compressed or uncompressed) and increasing the robustness and reliability, etc. Blind techniques play an essential role in many areas, including: forensic investigation, criminal investigation, surveillance systems, intelligence services, medical imaging, and journalism. Existing blind techniques have their limitations. For example, these techniques requirement many prior images to estimate the intrinsic patterns, which is a serious bottleneck (i.e., in potential situations only one image is provided) (Chen *et al.*, 2008; Swaminathan *et al.*, 2008).

To solve the above limitations, the present research work uses the capturing device (camera) statistical characteristics to detect forgery in digital images. The main goal is to develop single classification model that distinguishes tampered images from authentic images that does not require the original images or embedded detection techniques like digital watermarks. To achieve this primary goal, the following detailed objectives were formulated as listed below.

- To develop photomontage (image slicing) forgery detection algorithms that are robust in terms of
    - operations like resize, deform and rotate and no change and
    - Shapes like rectangle, triangle, circle and arbitrary
    - Contents like scene, animal, architecture, character, article, plant, nature and texture.
- To extract camera statistical features for camera pattern discovery
- To analyze the application of two single class classifiers, namely, Radial Basis Function based classifier and Support Vector Machine based classifier, for detecting tampering forgery
- To conduct performance evaluation to analyze the efficiency of the proposed classifiers in identifying tampered and authentic images

1.8. LAYOUT OF THE THESIS

The underlying objective of this research work is to identify tampered and authenticated images. This chapter provided an introduction to the topic, along with the methods used in this thesis to meet the research object. This chapter also outlined the motivation and objectives of the research. The rest of the dissertation is organized as follows.

Several researchers have addressed the problem of video annotation and the proposed techniques related to the present research work are given in **Chapter 2, Review of Literature.**

Chapter 3, Methodology, presents the techniques and methods used by the proposed tamper detection algorithm. A detailed description on the working of the algorithm is also presented in this chapter.

Chapter 4, Results and Discussion, analyzes and compares the performance of the proposed technique and compares it with the existing methods in terms of classification accuracy.

The concluding remarks and future extension work are described in **Chapter 5, Summary and Conclusion**.

The work of several researchers are quoted and used as evidence to support the concepts explained in this dissertation. All such evidences used are listed in the reference section of the dissertation.

Image tamper detection has become a predominant research field in image forensics. Out of the various methods of creating tampered images, photomontage or image slicing technique, have more popularity among forgers. The reason behind this is the easy creation process and advanced technology available today. The current need is to develop techniques to detect such forgeries and this research work proposes a technique for this purpose. However, the field has been probed by several researchers and the various previous techniques proposed are consolidated in the next chapter, Review of Literature.