7.1 Conclusion

Tampering images is not new. Availability of digital image technology and image processing software makes it easy for anyone to create a forgery. Not surprisingly, tampered images and videos are showing up everywhere, from courtrooms to scientific journals, and these images can have a profound effect on society. There is a clear need for tools to detect forgeries, and the field of digital image forensics has emerged to address this problem without any pre-requirements.

Five techniques for detecting different forms of tampering in manipulated digital images have been presented - Exact Block Matching Method and Robust Block Matching Method, JPEG Compression Analysis Method and Geometry Based Method. Detection of forgeries in digital video - Frame Duplication and Region Duplication detection have also been presented.

Although these techniques are different, they work under the assumption that tampering will alter some underlying statistical properties of natural/ original images. For each technique, the general approach has been the same: first, statistical changes associated with specific types of tampering are identified and quantified, then, detection methods are designed to estimate these changes and differentiate between tampered and unadulterated images.

Block based forgery detection algorithms are efficient in detecting Copy-Move forgery. Two methods namely Exact Match and Robust Match have been presented. Robust Match method yields a better result than the exact match. An improvement over the Robust Match has been made by reducing the number of features which resulted in the reduction of execution time without compromising its ability to detect forgery.

Most of the commercially available cameras store the images in JPEG format. Also, image tampering is always done using a photo-editing software. An image is first loaded into the photo-editing software, desired manipulations are performed, and then it is re-saved. If the tampered image is stored in JPEG format which is the default option
for most software, then the tampered image has been double compressed. It has been shown that when an image is double JPEG compressed specific correlations are introduced between Discrete Cosine Transform (DCT) coefficients of image blocks. The correlations have been quantified, and an algorithm that can distinguish between single and double JPEG compressed images has been devised. The algorithm has been tested on a large number of images and found that double JPEG compression is detectable for a range of quality factors. But if a tampered JPEG image is cropped prior to re-saving, the correlations described are not introduced. Also a double JPEG compressed image is not necessarily a forgery: for example, a user may re-save JPEG images with a lower quality to save storage space. Thus authenticity of a double JPEG compressed image is questionable and further analysis may be required.

Attempt has been made to detect forgery in images using geometric clues. Geometry based methods are extremely robust to compression, filtering, and other image processing operations. They are not dependent on the image format and can be used even when the quality of the image is low. Many techniques based on Principle Point, Shadows, Reflection and Perspective Constraints are possible. An algorithm based on Principle Point estimation was tried and limited success was obtained. However this endeavour will be continued to reach fruition.

Since video forgeries are becoming popular, effort was made to understand and design methods to detect them. Encouraging results have been obtained using correlation consistencies to detect frame duplication.

7.2 Future Avenues

Image forensics is a burgeoning research field and despite the limitations of existing methods, promises a significant improvement in forgery detection. It has made and will continue to make it harder and more time-consuming to create a forgery that cannot be detected.

Today’s technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago. Tomorrow’s technology will almost certainly allow us to manipulate digital media in ways that today seem unimaginable. As new techniques for exposing photographic frauds are developed, newer techniques
Conclusion and Future Avenues

will be developed to make better fakes that are harder to detect. While some of the forensic tools may be easier to fool than others, some tools will be difficult for the average user to circumvent.

However, two major issues must be addressed which can provide a congenial platform for a strong research to evolve:

1. Performance Evaluation and Benchmarking: The foremost concern that arises with respect to forensic use of proposed techniques is the achievable performance in terms of false-alarm and true-detection/identification rates and clear understanding of the factors that affect the performance. Many of the proposed techniques can be more accurately defined as proof of concept experiments. To further refine these methods, performance merits have to be defined more clearly and proper test and evaluation datasets have to be designed and shared.

2. Robustness Issues: The most challenging issue that image forensics research faces is the robustness to various common and malicious image processing operations. Proposed methods are not designed and tested rigorously to perform under the most difficult conditions. Since the information utilized by the image forensics techniques is mostly in imperceptible detail, it can be easily removed. It is a matter of time for such tools to be available for public use. Techniques have to be designed and evaluated with this caution in mind. Overcoming these challenges requires the development of several novel methodologies and thorough evaluation of their limitations under more general and practical settings. This can be achieved in collaboration with forensics experts and through their feedback on the developed methods.

Another interesting future research topic would be to investigate techniques for detecting tampering in digitally scanned images.

As the technology continues to evolve, it will become increasingly important for the science of digital forensics to keep pace and the never ending competition between image forgery creators and image forgery detectors continues.