CHAPTER 7

Our Contributions

In the following part we would like to highlight the salient contributions that we made through this study.

7.1 Accuracy of tampering detection and localization

Most of the earlier methods aimed that detection of tampering based on feature based hash generation. Precise localization of tampering is distinct advantage of algorithm used by us.

As mentioned in chapter 3, the sampling block which divides the image horizontally and vertically into a matrix form, is the fundamental area unit over which tampering localization is achieved. The absolute difference of the hash matrices corresponding to original and tampered images shows the area over one or more number of blocks. As a single hash value is assigned to each block a tampered area which is even lesser than a block size, will be shown over one full block. In such a case, if we reduce the sampling block size, we can narrow down the detected tampering region which is closer to actual tampered area. An iterative algorithm can be developed which automatically adjusts the sampling block size with variation of area of tampered region. This will depend on how accurately the size of tampering region is required to be found out.

Reduction in sampling block size will result in increased size of hash matrix and consequently length of hash vector. In certain situations, the length of hash
vector can be a limiting factor due to system requirements. In such cases, a trade-off between hash vector size and accuracy of tampering localization needs to be sought for.

7.2 Quantification of Robustness against CPM

One of the requirements of an efficient image tampering detection technique is robustness against content preserving manipulations such as low pass filtering (blur noise), minor contrast adjustment, brightness change and compression. The detection technique should be able to detect very minute structural tampering and at the same time, should be able to ignore content preserving manipulations mentioned above. Researchers have come out with algorithms which achieve both of these requirements. However, the critical level, up to which these manipulations will be ignored, has not been quantified in earlier works.

Generally, a typical tampering operation is limited to small part of the image while the content preserving manipulations are normally global in nature. It might just happen that quantity of content preserving manipulation summed up over full image, exceeds amount of malicious structural tampering which is limited to much smaller area. In that case, tampering index corresponding to content preserving manipulation will fall in category of malicious tampering. Therefore robustness should always be defined in terms of critical level of tampering above which CPM will be detected as malicious tampering.

In our work, we have identified the critical level of content preserving manipulations of each type. For example, in case of contrast change carried out through application of gamma correction, critical value of gamma has been found out up to which change in tampering index is very small and can be ignored. However, higher value of gamma, the resulting contrast change will enter the category of malicious tampering.
7.3 Similarity Value as measure of tampering

As mentioned above, a large number of techniques have been evolved to identify the tampered area in an image based on image feature extraction based hashing method. However, no serious effort has been made to give a mathematical index for amount of tampering. In this work, a quantitative index for amount of tampering called Similarity value as in eqn. (6.22) has been defined. It is very unique feature of our research work. It is a very suitable mathematical index because of two reasons.

1. It assumes values between 0 and 1 which is ideal to understand and use mathematically.

2. It varies with amount of tampering, assuming value 1 for non-tampered pair of images and 0 for completely dissimilar pair of images. In general it lies between 0 and 1 depending on amount of tampering.

7.4 Singular Value Decomposition for highly secure hash function

Properties of singular value matrix and orthogonal matrices in SVD were used to generate 2-level key based hash generation. It provided highly secure hash function specially suited to high security areas. Concept of 2-level key based hash is a novel method for tampering detection.

7.5 Use of Canny Edge Detector

So far, several techniques have been used for extracting the features of the image for hash generation. The basic requirement of an efficient hash generation technique are:

1. The technique should be extremely sensitive in detecting structural tampering so that even very minute tampering operations are picked up during
feature extraction and are suitably converted into hash value.

2. The technique should be able to ignore content preserving manipulations.

Canny Edge Detector meets both of these requirements very well. Firstly, it has efficient edge detection capability which provides very accurate image feature extraction. Double Edge Threshold method for picking or leaving an edge followed by Hysteresis Tracking for accepting/rejecting connected and disconnected edges respectively, provides very accurate representation of the image. This also ensures that content preserving manipulations are ignored as they normally lie below lower threshold level of Canny Edge Detector.

A very efficient hash function has been defined called “Average Edge Index” which is used to generate hash values for the blocks of image. This formulation has been defined and used for the first time in the field of image forensics. It is, therefore, a major contribution.

**7.6 Comprehensive Image Index**

Earlier researchers have used single feature of an image to generate hash value which is used to generate a hash matrix. This hash matrix is used for detection of tampering with respect to that particular feature. As discussed earlier, structural tampering is generally followed by brightness level tampering, contrast level tampering or both in order to hide structural tampering. To give a comprehensive measurement of this kind of multiple tampering, Comprehensive Image Index \((\eta_1, \eta_2, \eta_3)\) was defined and used successfully for various combination of tampering operations.

Concept of 3-tupled hash function for representation of image was used for the first time and therefore it is a very significant contribution.
7.7 An Image Tampering App

Based on our findings and results, we developed a plug-and-play type App for identification and localization of tampering in a suspect image against a given image. The situation, we may visualize, the Forensic Science Lab be given to identify whether a suspect image is tampered with or not. This App is so handy and easy to use which requires three steps:

1. Upload the original image
2. Upload the suspect image
3. Decide the block size (such as 50, 25, 20 etc.)
4. Click on ‘Result’ button to find the result and similarity value in no time.
Figure 7.1: The developed App which may make the FSL professional’s life easy.