PREFACE

Due to the rapid development of Internet technology, photo editing software packages, powerful computers and high resolution capturing devices, multimedia information in digital format such as document, graphics, drawings, still and moving images (video), audio can be easily spread, copied and edited. But ease of distribution and manipulation of digital data have also created a new class of problems such as protection of digital information from illegal duplication, manipulation, security and identification of rightful ownership. To tackle these problems, digital signatures, cryptographic methods and digital watermarking technique have emerged as solutions to tackle these problems. Cryptographic methods can protect content only in encrypted form, but once the content is decrypted then then the security gets breached. Digital signatures also have various disadvantages: 1) It encodes the signature in a file separate from the original image, thus require extra bandwidth to transmit; 2) it can only confirm whether the target image has been tampered but cannot indicate the exact location of tampered regions; 3) it cannot be used for tampered image restoration. On the other hand, watermarking schemes is used to protect the cover work in decrypted form. Hence, digital watermarking has drawn much attention of research community to resolve these demanding problems.

Digital watermarking is a technique that embeds imperceptibly a meaningful signature or some secret information called as the watermark, into the host or cover image. This imperceptible and secret watermark can be later detected/ extracted for a wide variety of purposes including authentication, content identification, copyright protection and ownership verification. The performance of the watermarking schemes can be measured by essential properties like fidelity, embedding effectiveness, robustness, imperceptibility, data payload and blind or informed detection etc. The relative significance of each property is dependent on the requirements and nature of the application. The fidelity of a watermarking scheme refers to the perceptual

similarity between the original and watermark versions of the cover image. The embedding effectiveness means the probability that the embedding procedure will successfully insert a watermark in arbitrarily selected cover work. In other word, the embedding effectiveness is probability of recognition imminently after embedding. Robustness of the watermark system refers to the ability to resist different image processing attacks. Imperceptibility refers to embedding of watermark into the cover image such that undetectable by a human perceptual system. Data payload refers to the number of bits a watermark encodes within a unit of time or within a cover image. For an image, the data payload would refer to the number of bits encoded within the image. In many application detection must be performed without access to the original work, so the detectors that do not require any information related to the original cover image are referred to as blind detector whereas opposite is called informed detector.

The main challenge of the watermarking schemes is to achieve a better trade-off among robustness, capacity and imperceptibility. Robustness can be achieved by increasing the capacity or strength of the embedded watermark, but the imperceptibility would decrease as well. Due to this trade-off, there is no general model of the content reconstruction problem and copyright protection despite the existence of the variety of watermarking schemes. Hence, digital image watermarking techniques for image authentication and copyright protection still remain unresolved or need to be improved, such as tamper localization accuracy, restored image quality, security, and false positive detection problem.

The objectives of this thesis are to develop effective watermarking schemes for image authentication and restoration as well as copyright protection. As already mentioned, the main problems related to the first application are low tamper localization accuracy, low restoration quality and inability to restore cover image at high tampering rate. The aim of this thesis is to address these problems by developing appropriate schemes for image authentication and restoration. Also the major problems regarding copyright protection are false positive problem, non-blind scheme,

unauthorized reading problem and computation of scaling factor. The second part of this thesis is dedicated in developing suitable watermarking schemes for copyright protection which address these issues.

The thesis can be divided in three parts. At the beginning, this thesis focuses on investigation the strength and limitations of current watermarking schemes. This thesis presents the comparative performance analysis of various watermarking methodologies along with the detailed discussion of significant existing watermarking schemes and their applications which are extremely diverse including authentication, restoration and copyright protection. The second part of this thesis focuses in developing an effective watermarking scheme that can be used for authentication, localization of the host image with high restoration capability. In this context, four new effective fragile watermarking schemes (Chapter 3, Chapter 4, Chapter 5, and Chapter 6) are proposed for tamper image detection and restoration. At end, a new robust and secure watermarking scheme (Chapter 7) is proposed in this thesis for copyright protection which is free from false detection problem. The overall thesis is organized into eight chapters as follows:

Chapter 1 presents a brief introduction of the problems addressed in this thesis followed by the objectives of the thesis. Finally the chapter concludes with a brief account on contributions of this thesis in the field of image watermarking scheme.

Chapter 2 discusses the theoretical background for digital watermarking scheme including its various properties, classification of watermarking schemes based on different criterion and various possible types of attacks. This chapter is also given an overview of Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Singular Value Decomposition (SVD) and Divisive Normalization Transform (DNT). Further, in this chapter extensive reviews of the significant literature in watermarking of digital images for copyright protection, authentication and restoration are presented along with their merits and demerits.

Chapter 3 presents block truncation coding (BTC) based self-embedding fragile watermarking technique for image authentication and recovery. The watermark is generated by quantization and BTC of each 2×2 block size and embedded into the three least significant bits (LSBs) of corresponding mapped block. Recovery bits are derived from the most significant bits (MSBs) of host image whereas authentication bits are derived from recovery bits, spatial location and secret key. This scheme is efficient in time complexity due to use of BTC and simple XOR operations only. The quality of the watermarked images is high, with the average of 39.0 dB PSNR. In process of watermark bits generation and embedding, small non overlapping blocks sized 2×2 are used to improve the accuracy of localization. Experimental results demonstrate that the accuracy of tampered detection and localization is effectively high and the recovery quality scores of the proposed scheme are better than the other existing state of art approaches.

Chapter 4 presents DCT based an effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability. This scheme has extreme localization and restoration capability. For each 2×2 non- overlapping block, two authentication bits, and ten recovery bits are generated from the five most significant bits (MSBs) of pixels. The recovery bits are generated by 5 MSBs–planes using DCT and quantization matrix $Q = \begin{bmatrix} 16 & 11 \\ 12 & 12 \end{bmatrix}$. Authentication bits are embedded in the three least significant bits (LSBs) of the block itself while recovery bits are embedded in the three LSBs of the corresponding mapped block. The accuracy of localization is extreme and blocking artifacts negligible in this scheme because of using the small blocks of size 2×2. The 5 MSB-layers of the tampered image can still be recovered with high accuracy up to 50 % tampering rate.

Chapter 5 also presents DCT based an effective self- recoverable fragile watermarking scheme. In this scheme, the cover image is divided in size of 2×2 non-overlapping blocks. This scheme uses two levels encoding for content restoration bits generation. For each block twelve bits watermark are generated from the five most significant

bits (MSBs) of each pixel and are embedded into the three least significant bits (LSBs) of the pixels corresponding to the mapped block. The principal content of tampered image can still be restored with high accuracy up to 50 % tampering rate.

Chapter 6 presents an efficient watermarking scheme for image authentication and localization with two chances for restoration capability. In this proposed scheme, the host image is divided into non-overlapping blocks of size 2×2. For each block, ten restoration bits and two authentication bits are generated from the five most significant bits (MSBs) planes. In the watermarked image each block contains restoration bits of other two partner blocks and authentication bits itself. These way two copies of restoration bits for each block are embedded into the host image. Therefore, we will get the second chance for block restoration in the case of one copy is destroyed. The proposed scheme is also effective because the authentication of each block is done by three-level hierarchical tampered detection mechanisms. So the authentication of each block can be ensured with high probability. The proposed scheme is capable to restore with high quality up to 50 % tampering rate from attacks like object removal, object addition and cropping.

Chapter 7 presents a DWT-SVD and DCT with Arnold Cat Map encryption based robust and blind watermarking scheme for copyright protection. The proposed scheme is free from false positive detection problem which normally occurs in the SVD-based watermarking schemes. Another major advantage of proposed scheme is that it is a blind scheme. So, there is no requirement of original watermark and cover image for watermark extraction. There is also no requirement to choose the scaling factor. Therefore, the proposed scheme is free from drawback related to the computation time for finding scaling factors. The scheme performed well against comprehensive set of attacks, proving its efficacy over other existing state of art approaches.

In **chapter 8**, the overall contribution of the thesis along with its future enhancements have been enlisted which might be of interest for further research in future.