Chapter 1

Introduction

With the advent and popularity of Internet and advancement of editing software, illegal operations such as duplication, modification, forgery have become very easy. These operations are not only difficult to prevent but also infringe the proprietary rights of the owners and reduce motivation for their creation. Therefore it has become an important issue to protect the intellectual property rights of digital media. Digital watermarking is the most typically used method of all the methods that have been proposed to protect intellectual property rights [1, 2]. The sudden increase in watermarking interest is most likely due to the increase in concern over copyright protection of content and the issue of rightful ownership. The first technology of copyright protection is cryptography where the content is encrypted prior to delivery and a decryption key is offered only to those who have purchased legitimate copies of the content. In addition, cryptography can protect content from manipulation only in encrypted form but once decrypted, the content has no further protection from illegal duplication. Watermarking schemes can be introduced in effort to tackle these increasing considerations. It is a technique that employs to guard digital content from illegal copying and manipulation even after it is in decrypted form. A watermark can be designed to survive encryption, decryption, compression, digital-to-analog conversion, file format changes etc.

Digital watermarking is one such technique that embeds imperceptibly secret information into the host image for authenticating, information hiding and copyright

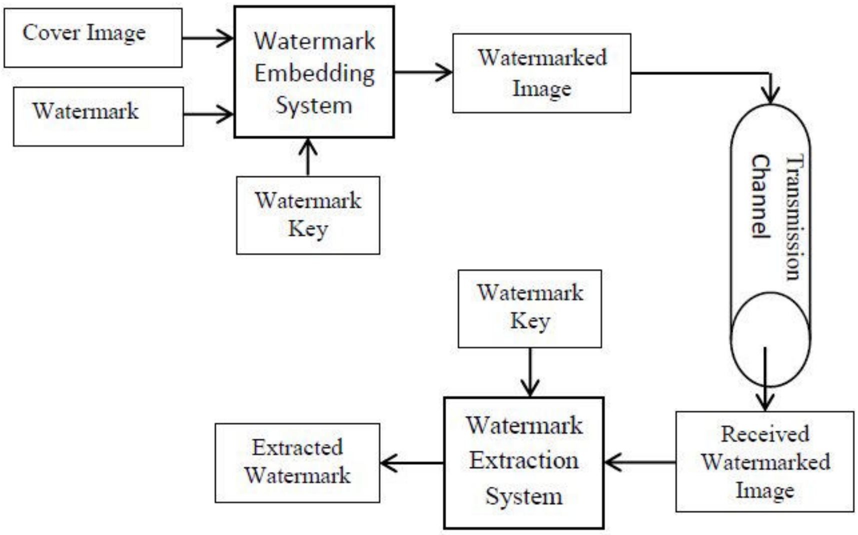

Figure 1.1: Block diagram of a basic watermarking model.

protection purposes. This secret information is extracted later for the authenticity and (or) to prove ownership of the cover image [3, 4]. The basic watermarking system (as shown in Figure 1.1) consists of an embedding system and a extraction system. There are three inputs for embedding system, first one is the host image and the second one is the watermark which is embedding into the host image. The third input 'watermark key' decides how to embed that watermark. The output of embedding system works as the input for the extraction system. Using the watermark key, through extraction system we try to determine whether watermark is present and decode the embedded message.

1.1 Motivation

The motivation of this thesis can broadly divided in two parts based on the applications of the watermarking. These are mentioned as follows.

1.1.1 Image authentication and restoration

Previous watermarking schemes in this application suffered from few problems which decreased the effectiveness of the watermarking techniques in one way or another.

The primary problems are low tampered localization accuracy, low restoration quality of the cover image and inability to restore at the high tampering rates. Increasing the localization accuracy would result in pin-pointing smaller possible regions during tampered detection which would ultimately increase the efficiency (running time) of the watermarking scheme. Secondly, a high restoration quality would increase imperceptibility between the recovered image and the original image (which is a very desirable property). Finally, accurately recovering the cover image from the tampered image subjected to a high tampering rate is essential requirement of any watermarking scheme.

1.1.2 Copyright protection

Watermarking schemes suited for copyright protection also suffer from some problems. These are false positive problem, non-blind scheme, unauthorized reading problem and computation of scaling factor. The first problem (false positive detection) refers to ability to extract an un-embedded watermark from the digital cover image. This results in ambiguity in validating the rightful owner. Non-blind schemes are those that require the original cover image during the watermark extraction process. Blind watermarking scheme has a great significance and practical value in many applications where keeping a copy of the original cover image without security is not practical. Another common security challenge that is related to watermarking schemes is keeping the secrete message (watermark/owner information) unreadable and un-understood for unauthorized persons. This is known as the unauthorized reading problem. Finally, computing the scaling factor is a very computationally exhaustive step. The temporal efficiency schemes which eliminate this redundant step are very much the need of the hour.

1.2 Thesis objectives

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.

1.3 Thesis contribution

In this thesis the fragile watermarking schemes for image authentication as well as robust digital image watermarking schemes for copyright protection are studied. The objectives of this work are to develop novel image watermarking schemes providing a performance enhancement over the other prior watermarking schemes. The aim of this thesis can be divided in three parts. At the beginning, this thesis is focused 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. To overcome the limitations of existing schemes, second part of this thesis focuses on developing effective watermarking schemes that can be used for authentication, localization of the host image with the restoration capability. In this context, four new effective fragile watermarking schemes (Chapter 3, Chapter 4, Chapter 5, and Chapter 6) are proposed for image authentication 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 key points addressed in this research include the following:

1. Develop and implement a new and effective self-embedding fragile watermarking scheme for image authentication and restoration by using block truncation coding.

2. Develop and implement a new and effective self-embedding fragile watermarking scheme for image authentication and restoration by using discrete cosine transformation with quantization matrix.

3. Develop and implement a new and effective self-embedding fragile watermarking scheme for image authentication and restoration by using discrete cosine transformation.

4. Develop and implement a new and effective self-embedding fragile watermarking scheme for image authentication, localization with two chance restoration capability.

5. Develop and implement a new and effective robust watermarking scheme for copyright protection by using discrete wavelet transform, singular value decomposition and discrete cosine transformation.

1.4 Thesis organization

The remainder of this thesis organized as follows:
Chapter 2 discusses the theoretical background for digital watermarking scheme its various properties, classification of watermarking schemes based on different criterion and various possible type of attacks. This chapter is also given an overview of Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Singular Value Decomposition (SVD) and. 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 x 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 performance of the proposed scheme is better than that of previous techniques. 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 object removing, object adding and cropping attacks.

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.