SYNOPSIS

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original. With digital multimedia distribution over World Wide Web, Intellectual Property Right (IPR) are more threatened than ever due to the possibility of unlimited copying. One solution would be to restrict access to the data using some encryption technique. However encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. This idea is implemented in bank currency notes. In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same “watermarking” concept may be used in multimedia digital contents for checking the authenticity of the original content. So, A Watermarking is adding an “ownership” information in multimedia contents to prove the authenticity. This technology embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected. Continuous efforts are being made to device an efficient watermarking schema but techniques proposed so far do not seem to be robust to all possible attacks and multimedia data processing operations. Considering the enormous financial implications of copyright protection, there is a need to establish a globally accepted watermarking technique. The sudden increase in watermarking interest is most likely due to the increase in concern over IPR. Today, digital data security covers such topics as access control, authentication, and copyright protection for still images, audio, video, and multimedia products. A pirate tries either to remove a watermark to
violate a copyright or to cast the same watermark, after altering the data, to forge the proof of authenticity. Generally, the watermarking of still image, video, and audio demonstrate certain common fundamental concepts. Numerous watermarking applications reported in the literature depend on the services we wish to support. Thus watermarking techniques may be relevant in various application areas including Copyright protection, Copy protection, Temper detection, Fingerprinting etc.

Based on their embedding domain, watermarking schemes can be classified either as Spatial Domain (The watermarking system directly alters the main data elements, like pixels in an image, to hide the watermark data) or Transformed Domain (the watermarking system alters the frequency transforms of data elements to hide the watermark data). The latter has proved to be more robust than the spatial domain watermarking.

To transfer an image to its frequency representation, one can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the least significant bit (LSB) values. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients. In 1997 Cox et.al presented a paper “Secure Spread Spectrum Watermarking for Multimedia”, one of the most cited paper (cited 2985 times till April’ 2008 as per Google Scholar search), and after that most of the research efforts are based on this work. Even though spatial domain based techniques can not sustain most of the common attacks like compression, high pass or low pass filtering etc., researchers present spatial domain based techniques too.

Since, financial implications of some of the application areas like fingerprinting and copyright protection are very high and till now no successful algorithm seem to be available to prevent illegal copying of the multimedia contents, the primary goal of this thesis work is chosen to develop watermarking schemes for images (which are stored in spatial domain as
well as transformed domain) which can sustain the known attacks and various image manipulation operations. This thesis resolves the following issues:

ISSUE 1: Till now there in no “Generic” nature in the watermarking algorithms available. More precisely, if certain approach is applicable for a gray level image, the same approach does not work for the other formats of an image.

ISSUE 2: Even if gray color image watermarking algorithms are extended for RGB color images, the maximum work has been done for BLUE color channel only because human eyes are less sensitive to detect the changes in BLUE color channel. No attack impact analysis, i.e, which color channel may be affected by a particular attack, has been carried out.

Therefore, apart from choosing digital Image Watermarking as a major problem, we have chosen to identify the suitability of a color channel with respect to attack (if any) for multi-color channel images (True color windows BMP, uncompressed JPEG). We also decided to explore the ways such that attack impacts may be minimized before the watermark embedding process.

ISSUE 3: In most of the research papers, once the watermarking scheme is finalized, it is applied to all test images. Since each image is different and has certain characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics.

Therefore we have decided to explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.

ISSUE 4: Mostly watermarking schemes are developed in a way that first a scheme is developed based on the extension of earlier presented one and then check its performance against the common image manipulations and known attacks. There are huge financial implications of watermarking schemes (say fingerprinting), but no scheme has been
developed, which is, by design, resistant to at least one attack, to ensure that, a particular attack (having most financial issues) cannot be conducted by an attacker.

Therefore we decided to design watermarking schemes such that an inherent nature in can be embedded to guarantee that at least one serious attack having most financial implications cannot be conducted on watermarked images.

If owner identification applications place the same watermark in all copies of the same content, then it may create a problem. If out of n number of legal buyer of content, one starts to sell the contents illegally, it may be very difficult to know who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy. Now if owner finds an illegal copy, he/she can find out who is selling his contents by finding the watermark, which uniquely belongs to a singly legal buyer. This particular application area is known as fingerprinting and thus has numerous financial implications. The most serious attack for fingerprinting is the “collusion attack”. If attacker has access to more than one copy of watermarked image, he/she can predict/ remove the watermark data by colluding them. Researchers working on “fingerprinting” primarily focus on the “collusion attack”.

So, while designing a watermark scheme, we decided that our proposed schemes must be designed in such a way that schemes are inherently collusion attack resistant. Therefore this thesis presents a new term “ICAR (Inherently Collusion Attack Resistant)” as a requirement for a watermarking system. The other 3 issues are taken into account while developing the watermarking schemes.

The first chapter is devoted to the introduction of the watermarking area. Data hiding background is represented and the related terminologies are explained. Then various application areas of watermarking are represented and what may the key requirements of a successful watermarking system are discussed. Since watermarking can be classified on
various parameters, the various types of watermarking are represented based on different classifications. The chapter-wise organization of the thesis is described.

The purpose of chapter-2 is to provide an overview of the existing watermarking techniques and related emerging issues and then problem statement formulation based on the current demand of the technology. In this chapter, apart from giving more emphasis only to those papers, which are related to this thesis work, care has been taken to cover more and more upcoming concepts. After then the shortcomings and the opportunities for the research work are identified and based on those the research issues are developed by giving proper justifications.

Chapter 3 describes the concepts like JPEG compression, which are the preliminaries requirements. We are using Peak Signal to Noise ratio (PSNR) and Correlation coefficient (CC) to measure the quality of the watermarked images and the extracted watermark logo, which are also described in this chapter. Finally the test images (both stored in spatial and transformed domain, gray and full colored) used in this thesis are given.

Our research work description starts from chapter 4. This chapter deals the watermarking of the gray images. To start with, initially we focus how we can increase the robustness of the well-known DCT and DWT based watermarking algorithms against some specific attacks. We present a new concept of “preprocessing” to increase the PSNR value of extracted logo from watermarked image if watermarked image has been attacked by JPEG compression attack. Preprocessing steps change or modify the original image such that, the affect after the attack on the watermarked image could be minimized. We tried to accomplish this by creating the same effect in an image, before watermarking it, which this image shall have, after it has been attacked. It is found that preprocessing steps increase the robustness of the watermarking scheme. Since DCT based schemes are robust against those attacks, which do not alter the perceptual quality of the image, we tested the proposed concept in the case of such attack, which has serious impact on the perceptual quality of the image. Therefore, we have extended the same hypothesis to increase the robustness against “Histogram equalization” attack, which attacks on perceptual quality of the image. Our results favor the
proposed hypothesis and show the importance of the attack impact analysis to increase the performance of the watermarking algorithms. After this, a watermarking scheme for gray level images is developed which is ICAR in nature as well as very robust against common image manipulation and attack (specially JPEG compression attack). The proposed scheme is developed over the classical middle-band coefficient exchange scheme to inherit its robustness against JPEG compression because this scheme takes the advantage of Human Visual System (HVS). We achieve ICAR nature using randomness and redundancy in coefficient exchange criterion. Apart from this, coefficient exchange criterion is develop to be dependent on low frequency coefficients to provide extra robustness because we know that any kind of attack or image manipulation can not alter the low frequency coefficients as this will have a serious impact on the image quality. Results indicate that, this scheme is, not only collusion attack resistant and resistant to common image manipulations and attacks, but more robust against JPEG compression attack as compared to other similar, state-of-art, watermarking schemes.

Chapter-5 deals with the watermarking of colored images. Colored images contain three color channel (red, green and blue), and human eyes are least sensitive to detect the changes in blue color channel and therefore most of the research work is based on hiding the watermark data in blue color channel. We propose that the suitability of the color channel is also dependent on the attack, the watermarked images have to undergo. For this we use 4 test images in Window’s 24-bit image format and analyze the robustness against JPEG compression attack by hiding the watermark data in all color channels. Results indicate that there is a strong connection between the color channel selection and the robustness against certain attack. It is found that for DCT based watermarking scheme, if we hide the watermark data in green channel, the robustness against the JPEG compression increases. The idea of preprocessing (proposed in previous chapter for gray level images) is also verified for color images. We then developed an ICAR watermarking scheme for colored images also, based on the scheme developed in chapter-4. We discovered that even after some serious attacks, one cannot change the average of all middle band coefficients of 8x8 DCT. We used this fact in hiding the watermark data. Again, being an ICAR scheme, this scheme is collusion attack resistant as well as very robust to common image manipulation.
We have tested test images against uniform scaling, brightness adjustment, Gaussian blurring, Hue and saturation along with malicious attack like histogram equalization and adding Gaussian noise. The proposed watermarking scheme sustains all attacks. In case of performance against JPEG compression, proposed scheme outperforms other similar watermarking schemes by giving very good results even at JPEG quality factor Q=5 (Compression ratio 98% and more), whereas other state-of-art watermarking schemes start loosing its robustness below the JPEG quality factor Q=20.

Chapter-6 describes the watermarking of JPEG image. Since, most of the images present on World Wide Web are in JPEG format, which is a highly compressed image format and stores the images in the transformed domain, we developed an ICAR watermarking scheme for JPEG images also.

Since JPEG is a very high compressed format, we know that while processing and storing a JPEG image, lot of its coefficients will change their values and thus recovery of the watermark data is difficult if only the relative strengths of coefficients of middle band regions are considered. Therefore, we provide extra robustness (by involving some coefficients whose values don’t changes much) by incorporating the large value at the top-left corner, the DC coefficient in 8x8 block DCT. This DC coefficient is the major dominating value while decompressing. This DC value alone can regenerate a very good approximated image by taking the IDCT. If this value is altered, the image is largely affected. We hide the watermark data based on DC coefficient. Proposed scheme is not only an ICAR scheme, but also enhances the performance. Results indicated that, the proposed scheme recovers the watermark even from highly attacked images which are compressed up to quality factor Q=5 of JPEG. In addition to this, the proposed scheme is resisting common image manipulations like cropping, scaling, flipping, histogram equalization, brightness- contrast adjustment, Hue-saturation alteration and Gaussian noise. In this chapter, we also explore a relationship between the robustness and some image characteristics. We experiment the standard deviation of an image and related this measure with the performance of the watermarking scheme.
After successfully developing the ICAR watermarking schemes for gray, colored BMP image and JPEG images using DCT, we explored the DWT. The basic need behind this is the upcoming JPEG2000 format. This image format stores the image using wavelet transform. Any of the image watermarked using our proposed algorithm may have to undergo JPEG2000 format conversion also, therefore to make the watermark embedding liner to the possible attack, we decided to use the DWT as embedding domain. A DWT based watermarking scheme may not sustain those attacks which a DCT based scheme can sustain very well (like JPEG compression), therefore we used the idea of Dual Watermarking, ie embedding the watermark using both DWT and DCT to increase to number of possible attacks which our watermarking scheme could sustain. Like our earlier proposed watermarking schemes, apart from ICAR in nature, the proposed DWT based watermarking scheme is very robust against .jp2 conversion attack (JPEG2000 format), JPEG compression, and other common image manipulations and attacks.

In Chapter-7, summary of the results and goal achieved, are given in detail. Future work of research work is also discussed. In the end, a list of all publications referred is given.

Keywords: Intellectual Property Right, Digital Image Watermarking, Collusion attack, Discrete Cosine Transform, Discrete Wavelet Transform, Haar wavelet, JPEG image encoding, Peak Signal to Noise Ratio, Correlation coefficient, JPEG2000 image encoding.