Chapter 67
Improving the Security of Digital Images in Hadamard Transform Domain Using Digital Watermarking

V. Santhi
VIT University, India

D. P. Acharjya
VIT University, India

ABSTRACT

In recent days, due to the advancement in technology there are increasing numbers of threats to multimedia data which are floating around in the Internet especially in the form of image data. Many methods exist to provide security for digital images but transform domain based digital watermarking could be considered as a promising method. Many transformation techniques are used to insert watermark in cover data, but this chapter deals with watermarking approaches in Hadamard transform domain. In traditional watermarking approaches the scaling parameter is empirically considered for inserting watermark but to maintain the quality of underlying cover images it needs to be calculated based on the content of the cover images. In order to make the watermarking algorithm completely automated the embedding and scaling parameters are calculated using the content of cover images. Many methods are existing for calculating scaling parameter adaptively but this chapter discusses various approaches using computational intelligence to arrive at optimum value of scaling and embedding parameters.

INTRODUCTION

With the advent of the Internet, the proliferation of images is creating a pressing need for copyright enhancement schemes that protect copyright ownership. The development in technologies make information processing relatively simple and quick but at the same time the rate of exposure to various attacks is very high due to the availability of tools and software as stated in Hartung and Kutter (1999) and Potdar et al

DOI: 10.4018/978-1-5225-0983-7.ch067

(2005)'s work. Protecting copyrights of digital images or any other multimedia data becomes challenging and to accomplish the same various security mechanisms have been developed including cryptography, steganography and digital watermarking. Cryprographic techniques could be used to protect digital data during transmission between sender to the receiver as described in Langelaar et al (2000)'s and Macq and Quisquater (1995)'s work. Steganography could be used for secret communication between trusted parties with the limitation of payload stated in Anderson and Petitcolas (1998)'s work. Thus digital watermarking is the elegant and most promising method to protect copyrights of image data. Based on human perception the existing watermarking schemes could be classified into visible and invisible watermarking schemes. Based on working domain digital image watermarking techniques could be classified as spatial domain and frequency domain techniques. Many works are existing in both working domains, out of which watermarking in spatial domain includes works of van Schyndel et al (1994), Langelaar et al (1997), Iftekharuddin and Frigui (2009) and Luo et al (2010). In general these spatial domain methods are fragile to image/signal processing operations or other attacks.

The other kind of watermarking techniques are transform domain technique in which watermark is embedded by modulating the magnitude of transform coefficients and provide robust watermarking schemes against common attacks. Different transformation techniques are used to transform an image intensity samples into frequency components include, Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT), Discrete/Fast Fourier Transform (DFT/FFT), Hadamard Transform (HT). Similarly, singular value decomposition (SVD) could also be used in digital watermarking field and its basics could be found in description of Andrews and Patterson (1976). Hadamard transform coefficients have components equivalent to many DCT low frequency AC coefficients in middle and high frequency bands. Out of all the transformation techniques, Hadamard transformation is considered as suitable for watermarking in high noise environment. Thus Hadamard transform based watermarking schemes are discussed in this chapter elaborately due to its simplicity. In the subsequent sections, literature review for both visible and invisible watermarking is presented.

REVIEW OF VISIBLE WATERMARKING SCHEMES

According to human perception watermarking fall into two categories: visible and invisible. Visible watermarking is predominantly used to identify the ownership and protect copyrights of digital images. It also prevents unauthorized use of copyrighted images as stated in Yeung et al (1997)'s work. Visible watermarking could be classified into two types namely reversible and irreversible watermarking. In reversible watermarking (Yang et al., 2009), the original signal is recovered after the removal of watermark but in irreversible watermark (Braudaway et al. 1996) the original signal could not be recovered after the removal of watermark.

Initially, the IBM digital library section has used a visible watermarking technique to watermark the digitized pages of manuscripts from the Vatican archive by Braudaway et al (1996). The watermarking method embeds watermark by modifying pixel luminance values and hence considered as spatial domain visible watermarking scheme. In this work, a bright pixel is darkened / brightened or a dark pixel is darkened / brightened by perceptually equal amount. Rao et al (1998) proposed automatic visible watermarking of images using the measurement of image texture to automate the adjustment of watermark intensity through a linear regression model. Lin and Chen (2000) have proposed a visible watermarking mechanism to embed a gray level watermark into the cover image based on a statistic approach. First,