Chapter 1
Realization of a New Robust and Secure Watermarking Technique Using DC Coefficient Modification in Pixel Domain and Chaotic Encryption

Shabir A. Parah
University of Kashmir, India

Nilanjan Dey
Techno India College of Technology, India

Javaid A. Sheikh
University of Kashmir, India

G.M. Bhat
University of Kashmir, India

ABSTRACT

The proliferation of information and communication technology has made exchange of information easier than ever. Security, Duplication and manipulation of information in such a scenario has become a major challenge to the research community round the globe. Digital watermarking has been found to be a potent tool to deal with such issues. A secure and robust image watermarking scheme based on DC coefficient modification in pixel domain and chaotic encryption has been presented in this paper. The cover image has been divided into 8×8 sub-blocks and instead of computing DC coefficient using Discrete Cosine Transform (DCTI, the authors compute DC coefficient of each block in spatial domain. Watermark bits are embedded by modifying DC coefficients of various blocks in spatial domain. The quantum of change to be brought in various pixels of a block for embedding watermark bit depends upon DC coefficient of respective blocks, nature of watermark bit (0 or 1) to be embedded and the adjustment factor. The security of embedded watermark has been taken care of by using chaotic encryption. Experimental investigations show that besides being highly secure the proposed technique is robust to both signal processing and geometric attacks. Further, the proposed scheme is computationally efficient as DC coefficient which holds the watermark information has been computed in pixel domain instead of using DCT on an image block.

DOI: 10.4018/978-1-7998-1763-5.ch001

1. INTRODUCTION

The advancement in communication and networked and multimedia technologies and exponential rise in the users of internet world-wide has resulted in reproduction and distribution of multimedia content likeaudio, images and videos easier. In such a protection of multimedia content has become one of the prominent issues. Various encryption techniques are being used to encrypt the multimedia information before actual data transmission to avert various security and Intellectual Property Right (IPR) problems. However, the disguised look of the scrambled data makes the attacker more suspicious and hence the chances of a malicious attack from the adversary get increased. Given the significance of the problem some serious work needs to be done in order to ensure security and maintain the easy availability of multimedia content. In recent years digital watermarking has received most attention for security and protect multimedia data (Cox et al, 1998; Djurovic et al, 2001; Parah et al, 2014a). A digital watermark is a special data such as logo, imperceptibly embedded in multimedia content like an image etc. to prove its ownership. Since images are one of the prominent members of multimedia content, most of the developed watermark schemes reported till date use images as cover media (Ghouti, et al, 2006). Depending upon visibility of watermark, watermarking schemes are classified into two classes viz.; visible and invisible techniques. Most generally invisible (imperceptible) watermarking is used for copyright protection. Ina typical imperceptible watermarking technique,the watermark or special information datais embedded inside a cover image in such a way that it is imperceptible. Thus, it does not catch the attention of human visual system and protectsthe cover image from common signal processing and geometric attacks. The aim is to create a watermarked image that looks precisely same to a human eye but ensures ownership claim whenever necessary. Digital watermarking has been successfully validated to be very suitable in identifying thesource; creator, owner and distributor of a digital multimedia object (Shih, 2008).

Digital image watermarking techniques are classified into various classes depending on various laid criteria. One of the prominent classifications is based on the domain of embedding the watermark. Based on this criteria watermarking is classified into spatial and transform domain (Shabir et al, 2013c; Parah et al, 2015d). Spatial domain watermarking techniques are the earliest and simplest. In spatial domain watermarking the watermark is embedded in some of the selected pixels (or all) of a cover image (Shabir et al, 2012b; Shabir et al, 2013c; Shabir et al, 2012c; Parah et al, 2015c). On the other hand, transform domain watermarking techniques involve modification of the transformed coefficients of the cover image. These transform domain watermarking makes use of various image transforms like Fourier Transform (FT) (Cintra et al, 2009; Liu and Zaho, 2010), Discrete Wavelet Transform (DWT) (Ghuti et al, 2006; Lu et al, 2012; Tsai, 2011; Wang et al, 2007), Singular Value Decomposition (SVD) (Djurovic et al, 2001; Lai and Tsai, 2010; Liu and Tan, 2002; Chen et al, 2013), Fractional Fourier Transform (FFT) (Bhatnagar and Ramman, 2011) and Contorlet transform. Pixel domain (spatial domain) watermarking schemes have least computational overhead; however they are fragile to various image processing and geometric attacks (Shabir et al, 2014a; Shabir et al, 2013a; Shabir et al, 2012a; Shabir et al, 2015; Shabir et al, 2014c). Transform domain methods on the other hand, are robust as compared to spatialdomain techniques. It is due to the underlying fact that when the inverse transformation is applied to a watermarked image, the watermark is irregularly distributed over the whole image. Thus it is very difficult for an attacker to extract or even modify the watermark. This paper presents a very intresting approach to watermarking, wherein we have successfully shown that a robust watermarking system can be implemented in spatial domain by embedding the watermark in DC component of Discrete Cosine Transfer (DCT) coefficients. Rest of the paper has been organised as follows. An extensive survey of