Chapter 1
Distributed Multiresolution Transform Based Framework for Watermarking

Gaurav Bhatnagar
University of Windsor, Canada

Jonathan Wu
University of Windsor, Canada

Balasubramanian Raman
Indian Institute of Technology Roorkee, India

ABSTRACT

In this chapter, a robust watermarking technique based on distributive multiresolution transforms (DMT) and singular value decomposition is presented to improve the protection of the images. First, the watermark image is mapped to another form to get reference watermark which is secret and only known to the owner/creator. In order to map watermark image into reference form, chaotic maps are used. The core idea of the proposed technique is to decompose host image via DMT followed by reference watermark embedding in DMT coefficients by modifying the singular values. After embedding, inverse transform is performed to get watermarked image.

DOI: 10.4018/978-1-61350-135-1.ch001

Two new different distributive multiresolution transforms, namely distributive multiresolution Fourier and distributive multiresolution cosine transform, are explored and used. The feasibility of the proposed method and its robustness against different kind of attacks are verified by computer simulations, and superiority is carried out by the comparisons with the existing methods.

INTRODUCTION

Nowadays, the substantial maturation of internet and web technologies have led to an environment in which some of very crucial issues for multimedia/digital media, particularly image, audio and video content, such as illegal copying, distribution, editing, copyright protection, authentication etc become very easy. This environment has led to an increasing demand for developing some standard solution to prevent these issues. As the possible solution, Cryptography (or encryption techniques) comes to our help. Cryptography is the art of secret (crypto) writing (graphy). It is the science of using mathematics to encrypt and decrypt data. Whilst the traditional cryptographic solutions can encrypt multimedia and transmit it across insecure channel so that it cannot be read by anyone except the authorized recipient. However they require the receiver to use a key to decrypt the data successfully. Moreover, such solutions do not prevent or track the content against illegitimate reproduction after it has been decrypted. It essentially provides end-to-end security while distributing digital media over a large variety of distributions systems. It is mainly concerned with the secured communication instead of ulterior copyright infraction and protecting the content of the message rather than their existence. As per their existence is concerned, a new terminology named steganography/data hiding comes into picture. Steganography (Katzenseisser & Petitcolas, 2000) is the art of covered (secret) writing (graphy). It enables hiding a message data into host multimedia such that there is no perceptual degradation in the host multimedia according to human perception. The composite multimedia is usually termed as the stego/marked multimedia. Unlike cryptography, steganography tries to conceal the existence of the messages. It typically relates only to covert point to point communication between two parties in other words it is a form of subliminal communication. The major drawback of steganographic techniques is the limited robustness against modification of the digital media, occurred during transmission, storage or file conversion. In order to take care of robustness problem, a new terminology named Digital Watermarking is identified as effective solution (Cox et al., 2001; Arnold et al., 2003). Thus, rather than steganography, digital watermarking is used wherever the intellectual property protection is concerned. The inserted/embedded message data is called watermark/signature/metadata whereas the multimedia to be protected is called cover-data (Muharemagic & Furht, 2004).