Chapter XII
A Content-Based Watermarking Scheme for Image Authentication Using Discrete Wavelet Transform Inter-Coefficient Relations

Latha Parameswaran
Amrita University, India

K. Anbumani
Karunya University, India

ABSTRACT

This chapter discusses a content-based authentication technique based on inter-coefficient relationship of Discrete Wavelet Transform (DWT). Watermark is generated from the first level DWT. An image digest (which is a binary string) is generated from the second level DWT. The watermark is embedded in the mid-frequency coefficients of first level DWT as directed by the image digest. Image authentication is done by computing the Completeness of Signature. The proposed scheme is capable of withstanding incidental image processing operations such as compression and identifies any malicious tampering done on the host image.

INTRODUCTION

With the proliferation of the Internet, distribution of digital multimedia has grown enormously in the recent years. Multimedia normally refers to data such as text, images, sound, video, graphics etc. With the availability of simple and economic tools, multimedia contents can be easily pirated...
A Content-Based Watermarking Scheme for Image Authentication

or altered either incidentally or intentionally. The low cost of reproduction, storage and distribution, also paves way for large-scale commercial infringement (Eskicioglu et.al 2003). Digital watermarking is one of the significant technologies available for multimedia security.

A digital watermark is a piece of information that is hidden in a multimedia content, in such a way that it is imperceptible to a human observer, but easily detected by a computer. The principal advantage is that the watermark is inseparable from the content (Cox et.al 2002). Digital watermarking is the process of hiding the watermark imperceptibly in the content. This technique was initially used in paper and currency as a measure of authenticity.

Digital Watermarking involves two major phases:

(i) Watermark embedding, and
(ii) Watermark extraction.

Digital watermarks can be a pseudo random sequence or a logo of a company or an image or content-based ie. features derived from the image itself. Watermark embedding is done in the watermark carriers such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT), etc of the original data resulting in watermarked data. The watermarked data may be compressed to reduce its size, corrupted by noise during its transmission through a noisy channel. It may be subjected to other normal image processing operations such as filtering, histogram modification etc. Also malicious intruders may tamper the data. Watermark extraction is on the received image. Metrics like correlation are used to verify the integrity of the received image.

Digital watermarking is a multidisciplinary field that combines media and signal processing with cryptography, communication theory, coding theory, signal compression and the theory of human perception (Dittaman 2001).

As watermarks are inseparable from its host data, they are suitable for several applications (Cox et. al 2002, Cox et.al 1999):

- Broadcast and publication monitoring
- Owner identification
- Copyright protection or proof of ownership
- Transaction tracking
- Content authentication
- Copy control

Content authentication is one of the applications of watermarking. The objective is to provide a method to authenticate the image and ensure the integrity of the image.

Authentication is quite independent of encryption. In encryption-based systems, the intent is to ensure the secrecy of a given data and to provide assurance that the received data has not been tampered or altered. In some cases, modifications on image may be unintentional and may not affect the content. In other cases, modifications may be intentional and may inadvertently affect the interpretation of the host image. For example, an inadvertent change in an X-ray image might result in misdiagnosis; similarly, malicious tampering of photographic evidence in a trial can result in wrong conviction or acquittal (Cox et. al, 2002, and Cox et.al, 1999).

In the context of content authentication, normal image processing operations like compression, filtering and noise are considered as legitimate, content-preserving modifications.

Other modifications on the image such as:

- Geometric transformations like rotation, scaling, translation etc,
- Cropping, and
- Addition or removal of objects from the host image are considered as illegitimate, malicious, content-changing and tampering.