A Semi-Fragile Image Watermarking Using Wavelet Inter Coefficient Relations

Latha Parameswaran, AMRITA University, India
K. Anbumani, Karunya University, India

ABSTRACT

Proliferation of multimedia on the Internet has led to the need for developing authentication mechanisms. This article proposes a new blind watermarking scheme based on the contents of the image in the discrete wavelet transform domain for image authentication. The host image is discrete wavelet transformed up to second level. The relationship between neighboring wavelet coefficients in each band of the second level decomposition is considered to construct the content-based watermark. The watermark is embedded in the first level mid frequency band, of the discrete wavelet transformed image. The received image is authenticated by extracting the watermark and determining the level of authenticity. This scheme is capable of tolerating content-preserving modifications and detecting content-changing modifications. Experimental results prove the efficiency of the scheme.

Keywords: discrete wavelet transform; image authentication; image digest

INTRODUCTION

Multimedia data is an important asset in all business operations, government or private. Therefore, it is important that these agencies should also maintain the integrity of the data and secure it. Technologies for capturing, storing, retaining, and accessing information are expanding the volume of information that can be acquired, with increased longevity. But the technology to secure multimedia data is still an open problem.

Authentication techniques provide a means of ensuring the integrity of a message. Authentication, in general, is quite independent of encryption, where the objective is to ensure the secrecy of a given message and not to hide the message.
Authentication systems are essentially designed to provide assurance that a received message has not been tampered with and the specified source is indeed the originator. The general model for authentication is shown in Figure 1. Image authentication can be achieved by digital watermarking.

A digital watermark is a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but can easily be detected by a computer. The principal advantage is that the content is inseparable from the watermark, making it suitable for several applications such as signature, fingerprinting, copy control, broadcasting, authentication, secret communication, and other areas (Cox, Miller, & Bloom, 2002).

The general image authentication model has a sender, an image \( X \) and a receiver. The sender computes an authenticated image \( Y \) and sends it to the receiver. The image \( Y \) is a function of \( X \) and an authentication key \( a \), \( Y = f(X \parallel a) \). The receiver verifies \( Y \) using a verification key which could be the same as the one used by the sender (private key) or a different key (public key). The authenticated image can be intercepted by any malicious attacker. The attacker may modify \( Y \) as \( Y' \) and send it to the receiver. Thus the receiver requires an authentication scheme to verify the integrity of the image (Stallings, 2002). Watermarking is a solution to ensure image integrity.

**Watermarking Characteristics**

Many watermarking schemes are available in the literature for image authentication. These watermarking schemes have specified a set of characteristics. Few characteristics of the watermark are (Cox et al., 2002; Miller & Cox, 1997):

- **Fidelity**: The watermark should be imperceptible to the viewer and should not degrade the quality of the content.
- **Robustness and tamper-resistance**: The watermark must be robust against common image processing operations such as blurring, noise addition, sharpening, and compression. It is also important that the watermark should survive geometric distortions such as translation, rotation, scaling, and cropping.

![General image authentication model](image)

\( X \rightarrow \) Sender \( Y \rightarrow \) Receiver \( X \rightarrow \) Authentic?

\( Y \rightarrow \) Attacker
Related Content

Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis  
[www.igi-global.com/chapter/information-security-policies-reduce-incidence/29060?camid=4v1a](www.igi-global.com/chapter/information-security-policies-reduce-incidence/29060?camid=4v1a)

Internal Auditing for Information Assurance  
[www.igi-global.com/chapter/internal-auditing-information-assurance/20658?camid=4v1a](www.igi-global.com/chapter/internal-auditing-information-assurance/20658?camid=4v1a)

PCI Compliance: Overcoming the Challenges  
[www.igi-global.com/article/pci-compliance-overcoming-challenges/34058?camid=4v1a](www.igi-global.com/article/pci-compliance-overcoming-challenges/34058?camid=4v1a)