Digital Image Protection using Keyed Hash Function

Siva Charan Muraharirao, Dhirubhai Ambani Institute of Information and Communication Technology, India

Manik Lal Das, Dhirubhai Ambani Institute of Information and Communication Technology, India

ABSTRACT
Digital image authentication is an essential attribute for protecting digital image from piracy and copyright violator. Anti-piracy, digital watermarking, and ownership verification are some mechanisms evolving over the years for achieving digital image authentication. Cryptographic primitives, such as hash function, digital signature, and message authentication codes are being used in several applications including digital image authentication. Use of Least Significant Bit (LSB) is one of the classical approaches for digital image authentication. Although LSB approach is efficient, it does not provide adequate security services. On the other hand, digital signature-based image authentication provides better security, but with added computational cost in comparison with LSB approach. Furthermore, digital signature-based authentication approach requires managing public key infrastructure. Considering security weakness of LSB-based approach and cost overhead of public key based approach, the authors present a digital image authentication scheme using LSB and message authentication codes (MAC). The MAC-based approach for authenticating digital image is secure and efficient approach without public key management overhead. The authors also provide experimental results of the proposed scheme using MATLAB. The experimental results show that the proposed scheme is efficient and secure in comparisons with other schemes.

Keywords: Digital Signature, Digital Watermarking, Image Authentication, Least Significant Bit (LSB), Message Authentication Codes (MAC)

1. INTRODUCTION
Recent advances of digital technologies make alteration of multimedia data simpler and undetectable by human audible-visual system (Darko & Borko, 2005). One of the primary reasons could be digital contents are easily accessible via Internet and can be replicated and redistributed by illegal means. Use of digital content with proper acknowledgement for academic purpose or non-profit business is a common practice. But, forging data, usage of someone data without due citation, tampering data and blackmailing someone credential, making money from stolen data, etc are major concerns in multimedia security. When a bad person is getting away by doing these practices without being caught then there are two important issues arise - on one hand, the bad person knows that s/he can enjoy her/his life in this

DOI: 10.4018/ijcvip.2012040103
way without expecting any punishments; and on the other hand, it is because of poor content protection and detection mechanism by the content owner. In other words, preventing bad persons from fabricating content and detecting both fabricated data and creator are challenging tasks in securing multimedia data. In order to protect multimedia data, some techniques such as digital watermarking, scrambling, authentication, integrity or a combination of these play an important role. This paper focuses one of the techniques, namely digital watermarking with cryptographic primitives.

Digital watermarking (Darko & Borko, 2005) is a technique that inserts a piece of information into a target image, which can be later extracted for a variety of purposes and/or detected in case of malpractices. A watermark can be a binary string, a logo, or some intended features of the multimedia content. Whatever maybe the watermark content, the watermarking technique needs to be designed in such a way that an unauthorized entity should not be able to identify any information about the watermarked content and position of it. Whereas, the content owner or authorized entity should be able to identify the watermarked information from the image as and when needed.

Watermarking techniques (Darko & Borko, 2005; Mandhani, 2003; Hwang, Chang, & Hwang, 1999) can be broadly classified in two categories: visible watermarking and invisible watermarking. Visible watermarking is the classical way of watermark generation, extraction and deletion, where the watermark is inserted into a cover object. Although visible watermarking is useful for identification purpose, it is not secure watermarking for applications such as image authentication, image alteration and copy protection. In contrast, invisible watermarking is the modern approach for digital image authentication and piracy detection. A typical process flow of embedding and extraction of digital watermark in an image is shown in Figure 1.

This paper aims to provide a secure scheme for digital image authentication using invisible watermarking technique. Many techniques (Walton, 1995; Mandhani, 2003; Tang, Hwang, & Yang, 2002; Hwang, Chang, & Hwang, 1999; Yeung & Mintzer, 1997; Wong & Memon, 2001; Chang, Hu, and Lu (2006) and Ahmed, Siyal, and Abbas (2010) have been proposed for protecting multimedia data, detecting content piracy and retaining copyright or ownership, where the protection features include data authentication, data integrity, data hiding, and so on. Least Significant Bit (LSB) and parity bit checking have been used in several products as a light-weight image protection mechanism (Walton, 1995; Mandhani, 2003). LSB technique makes watermark perceptually invisible and the quality of the image is preserved. The working principle of LSB technique is briefly explained as follows. For embedding process, every pixel in a gray-scale image is represented by a byte, or 8 bits. Each bit from the

Figure 1. Embedding and extraction of watermark
10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:
www.igi-global.com/article/digital-image-protection-using-keyed/72314?camid=4v1

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Computer Science, Security, and Information Technology. Recommend this product to your librarian:
www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

Thresholding Selection Based on Fuzzy Entropy and Bee Colony Algorithm for Image Segmentation
www.igi-global.com/chapter/thresholding-selection-based-fuzzy-entropy/75681?camid=4v1a

Human Face Recognition using Gabor Based Kernel Entropy Component Analysis
www.igi-global.com/article/human-face-recognition-using-gabor/74797?camid=4v1a

Construction of 3D Triangles on Dupin Cyclides
www.igi-global.com/article/construction-triangles-dupin-cyclides/55099?camid=4v1a
Visual Behavior Based Bio-Inspired Polarization Techniques in Computer Vision and Robotics
www.igi-global.com/chapter/visual-behavior-based-bio-inspired/77606?camid=4v1a