Chapter I
Authentication Watermarkings for Binary Images

Hae Yong Kim
Universidade de São Paulo, Brazil

Sergio Vicente Denser Pamboukian
Universidade Presbiteriana Mackenzie, Brazil

Paulo Sérgio Licciardi Messeder Barreto
Universidade de São Paulo, Brazil

ABSTRACT

Data hiding (DH) is a technique used to embed a sequence of bits in a cover image with small visual deterioration and the means to extract it afterwards. Authentication watermarking (AW) techniques use DH to insert particular data into an image, in order to detect later any accidental or malicious alterations in the image, as well as to certify that the image came from the right source. In recent years, some AWs for binary images have been proposed in the literature. The authentication of binary images is necessary in practice, because most scanned and computer-generated document images are binary. This publication describes techniques and theories involved in binary image AW: We describe DH techniques for binary images and analyze which of them are adequate to be used in AWs; analyze the most adequate secret- and public-key cryptographic ciphers for the AWs; describe how to spatially localize the alteration in the image (besides detecting it) without compromising the security; present AWs for JBIG2-compressed binary images; present a reversible AW for binary images; and finally present our conclusions and future research.

INTRODUCTION

This publication describes techniques and theories involved in binary image AW. The authentication of binary images is necessary in practice because most of scanned and computer-generated document images are binary. These documents must be protected against fraudulent alterations and impersonations.

Binary images can be classified as either halftone or non-halftone. Halftone images are binary representations of grayscale images. Halftoning techniques (Knuth, 1987; Roetling & Loce, 1994; Ulichney, 1987) simulate shades of gray by scattering proper amounts of black and white pixels. On the other hand, non-halftone binary images may be composed of characters, drawings, schematics, diagrams, cartoons, equations, and so forth. In many cases, a watermarking algorithm developed for halftone images cannot be applied to non-halftone images and vice versa.

DH or steganography is a technique used to embed a sequence of bits in a cover image with small visual deterioration and the means to extract it afterwards. Most DH techniques in the literature are designed for grayscale and color images and they cannot be directly applied to binary images. Many of continuous-tone DHs modify the least significant bits (Wong, 1998), modify the quantization index (Chen & Wornell, 2001), or modify spectral components of data in a spread-spectrum-like fashion (Cox, Kilian, Leighton, & Shamoon, 1997; Marvel, Boncelet, & Retter, 1999). Many of the continuous-tone DHs makes use of transforms like DCT and wavelet. Unfortunately, none of the previous concepts (least significant bits, quantization indices, and spectral components) are applicable to binary images. Binary images can be viewed as special cases of grayscale images and consequently can be transformed using DCT or wavelet, resulting in continuous-tone images in transform-domain. However, modifying a transform-domain image to insert the hidden data and inverse transforming it, usually will not yield a binary image. Hence, transforms like DCT and wavelet cannot be used to hide data in binary images. As consequence of the previous reasoning, special DH techniques must be designed specifically for binary images.

A watermark is a signal added to the original cover image that can be extracted later to make an assertion about the image. Digital watermarking techniques can be roughly classified as either *robust watermarks*, or *authentication watermarks*. Robust watermarks are designed to be hard to remove and to resist common image-manipulation procedures. They are useful for copyright and ownership assertion purposes.

AWs use DH techniques to insert the authentication data into an image, in order to detect later any accidental or malicious alterations in the image, as well as to certify that the image came from the right source. AWs can be further classified in two categories: fragile and semi-fragile watermarks.

Fragile watermarks are designed to detect any alteration in the image, even the slightest. They are easily corrupted by any image-processing procedure. However, watermarks for checking image integrity and authenticity can be fragile because if the watermark is removed, the watermark detection algorithm will correctly report the corruption of the image. We stress that fragile AWs are deliberately not robust in any sense. In the literature, there are many AW techniques for continuous-tone images (Barreto & Kim, 1999; Barreto, Kim, & Rijmen, 2002; Holliman & Memon, 2000; Wong, 1998; Yeung & Mintzer, 1997; Zhao & Koch, 1995). It seems to be very difficult to design a really secure AW without making use of the solid cryptography theory and techniques. Indeed, those AWs that were not founded in cryptography theory (Yeung & Mintzer, 1997; Zhao & Koch, 1995) or those that applied cryptographic techniques without the due care (Li, Lou, & Chen, 2000; Wong, 1998) were later shown to be unreliable (Barreto & Kim, 1999; Barreto et al., 2002; Holliman & Memon,