Available online at www.sciencedirect.com
SCIENCE DIRECT®
Signal Processing: *Image Communication* 20 (2005) 129–150
SIGNAL PROCESSING: IMAGE COMMUNICATION
www.elsevier.com/locate/image

Towards robust image watermarking: combining content-dependent key, moment normalization, and side-informed embedding

Chun-Shien Lu*

Institute of Information Science, Academia Sinica, Taipei, Taiwan 115, ROC

Received 25 March 2004

Abstract

In digital watermarking, robustness is still a challenging problem if different sets of attacks need to be tolerated simultaneously. In this paper, we deal with this problem by using an integrated solution involving side-informed embedding, moment normalization, and content-dependent watermarks. First, a new image watermarking method based on the concept of communications with side information is proposed. We investigate the characteristics of mean filtering in formulating new watermark embedding and extraction processes. Second, regarding resistance to geometrical attacks, we do not rely on the concept of pilot signals because they are vulnerable to synchronization removal attacks. We instead use block-based watermarking and moment normalization mechanisms to recover geometrical distortions. Third, regarding resistance to the copy attack, the content-dependent watermark is employed to avoid treating an un-watermarked image as one that has been watermarked. The robustness of our approach has been verified using both the StirMark and the copy attack.
© 2004 Elsevier B.V. All rights reserved.

Keywords: Attack; Content-dependent watermark; Moment normalization; Robustness; Side information; Watermarking

1. Introduction

Digital watermarking [12] is considered by many to be a helpful technology for copyright protection. Many requirements [5] have been recognized and evaluated with respect to the benchmarking of watermarking systems. Among them, some parameters (e.g., fidelity, robustness) are commonly used in a variety of applications, while others (e.g., high capacity, complexity) are only employed in specific applications. Due to many attacks already exist and new attacks will appear in the future, robustness is still definitely important.

In general, attacks can be roughly categorized into four classes [37]: (1) removal attacks that

*Tel.: +886 2 27883799 ext. 1513.
E-mail address: lcs@iis.sinica.edu.tw (C.-S. Lu).

0923-5965/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.image.2004.10.002

Nomenclature

$\mathbf{w}^{\text{ori}}$	the watermark before ECC
$w_{\text{len}}^{\text{ori}}/\lvert\mathbf{w}^{\text{ori}}\rvert$	the length/magnitude of $\mathbf{w}^{\text{ori}}$
$\mathscr{K}$	the secret key used to generate $\mathbf{w}^{\text{ori}}$
$\mathbf{w}$	the embedded watermark signal after ECC
w_{len}	the length of $\mathbf{w}$
$\mathbf{w}^{\mathbf{e}}$	the extracted watermark signal
$\mathbf{w}^{\mathbf{ecd}}$	the extracted watermark after error correction decoding of $\mathbf{w}^{\text{e}}$
$\lvert\mathbf{w}^{\mathbf{ecd}}\rvert$	the magnitude of $\mathbf{w}^{\text{ecd}}$
$Q(i)$	the magnitude of an embedded watermark value $w(i)Q(i)$
Q	the constant watermark magnitude
$f_i(j)$	the jth DCT coefficient in a block i
$f_i^h(j)/f_i^a(j)$	the jth modulated/attacked DCT coefficient in a block i
$u(i)$	the mean of the selected DCT coefficient in a block i
$\mathbf{U}$	the 1-D sequence of $u(i)$'s after secret key-based shuffling
$\bar{u}(i)$	the mean of $u(\cdot)$'s
$\bar{\mathbf{U}}$	the 1-D sequence of $\bar{u}(i)$'s
$d(i)$	the difference between $u(i)$ and $\bar{u}(i)$
$d(i)$'s, $\mathbf{v}$	the signal extracted from a cover image
$u^h(i)$	the modulated version of $u(i)$
$u^a(i)$	the attacked version of $u^h(i)$
$\bar{u}^h(i)/\bar{u}^a(i)$	the mean filtered version of $u^h(i)/u^a(i)$
$\bar{\mathbf{U}}^{\mathbf{h}}$	the watermarked version of $\bar{\mathbf{U}}$
$d^h(i)$	the modulation quantity
$d_{\text{HVS}}^h(i)$	the modulation quantity constrained by the human visual system
$d^h(i)$'s, $d_{\text{HVS}}^h(i)$'s, $\mathbf{s}$	the mixed signal
mf_{s}	the support for mean filtering
$\mathbf{c}$	channel fading
$c_i(j)$	an element of channel fading
$C(i)$	the mean of $c_i(j)$'s in block i
$\bar{C}(\cdot)$	the mean filtered version of $C(\cdot)$'s
$\mathbf{a}$	channel noise
$a_i(j)$	an element of channel noise
$A(i)$	the mean of $a_i(j)$'s in block i
$\bar{A}(\cdot)$	the mean filtered version of $A(\cdot)$'s
ρ	the normalized correlation
T	the threshold used to indicate the presence/absence of a watermark
CDK	the content-dependent key
CDW	the content-dependent watermark

contain non-geometrical modifications, including filtering, lossy compression, denoising, and sharpening; (2) geometrical attacks that contain local/global transformations, warping, and jitter; (3) protocol attacks that are mainly composed of the copy attack and the watermark inversion attack; (4) cryptographical attacks that are related to the security of keys, such as brute force key search and oracle attacks. Removal attacks are considered to be less challenging because earlier robust watermarking methods [12] could resist them to a certain degree. Consequently, geometrical attacks have recently been taken more seriously. In [33], Ruanaidh and Pun presented an RST (rotation, scaling, and translation) resilient watermarking scheme based on the Fourier–Mellin transform (FMT). The authors also noticed a weakness in that practical implementation suffers from numerical instability that results when the log-polar mapping[1] is inverted to get the watermarked image. To deal with this problem, Lin et al. [22] proposed the implementation of an inexpensive algorithm. Recently, another efficient implementation of the Fourier–Mellin transform developed by using logarithmic radial harmonic functions (LRHFs) to avoid interpolation artifacts has been proposed [10]. Despite the capability of those Fourier–Mellin transform-based watermarking methods to achieve RST invariance, their resistance to other geometrical distortions (e.g., changes of the aspect ratio and cropping) and removal attacks is limited because FMT is only RST invariant and most of the FMT information is contained in the phase instead of

[1]There existed another version that was based on log–log map, which could resist change of aspect ratio but is sensitive to rotation. Furthermore, it should be noted that FMT cannot recover from general affine transformations.

Download English Version:

https://daneshyari.com/en/article/10363151

Download Persian Version:

https://daneshyari.com/article/10363151

Daneshyari.com