International Journal of Innovative Computing, Information and Control
Volume **7**, Number **10**, October **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5893–5908

DS-CDMA-BASED WATERMARKING: A LOW-POWER, HIGH-SECURITY ALGORITHM FOR EMBEDDED SYSTEMS

Yu-Ting Pai, Li-Te Lee and Shanq-Jang Ruan

Department of Electronic Engineering
National Taiwan University of Science and Technology
No. 43, Sec. 4, Keelung Rd., Taipei City 106, Taiwan
{ D9402105; M9602101; sjruan }@mail.ntust.edu.tw

Received May 2010; revised September 2010

Abstract. *Digital watermarking is a technique that embeds invisible information into digital content to protect the intellectual property rights of the original digital content creator. In attempts to achieve greater levels of robustness, transparency and blindness of digital marking considerable research has been undertaken with most studies having proposed watermarking techniques with satisfactory resistance against most attacks. However, the complicated frameworks require large areas and high energy consumption requirement for hardware implementation. This paper presents an energy-efficient and robust watermarking algorithm based on Direct Sequence-Code Division Multiple Access (DS-CDMA), which is a low complexity architecture for embedded systems. Experimental results demonstrate that the proposed watermarking algorithm effectively reduces energy consumption and is able to survive various signal distortions.*

Keywords: Watermark, Blind, DS-CDMA, Embedded systems, Energy-Efficient, Robustness

1. **Introduction.** Owing to the rapid growth of Internet technology, people now can obtain multimedia information more conveniently than ever before. Consequently, digital content is more easily interpolated and pirated, which makes copyright infringement a widespread societal issue. Digital watermarking is a technique that allows the content creator to embed invisible information into their work to prevent unauthorized copying of digital content and therefore has become a topic of substantial interest.

Over the past few decades, many contributions have been made through hundreds of watermarking related publications [1-9]. Cox et al. argued that watermarking can resist signal processing attacks well by inserting data into the frequency domain [10]. Kii et al. used a patchwork that is robust against image cropping attacks [11]. Hsu and Wu's algorithm exploited a block-based permutation technique] to improve perceptual invisibility [12]. Fei et al. proposed an algorithm to improve resistance against compression [13]. Lu et al. exploited an efficient modulation strategy to improve robustness against several different kinds of attack [14]. All of the methods mentioned are non-blind watermarking schemes, which means that the original image is required for the extraction process. In recent years, however, research has instead focused on blind watermarking schemes, which are sophisticated algorithms for detecting watermarks without the need for the original image [15-17]. Wu and Hsieh adopted the zerotree of discrete cosine transform (DCT) to embed watermarks [18]. Sun et al. proposed an algorithm based on the General Gaussian Model [19]. Yu and Chen presented a blind watermarking scheme using quantization and voting policies [20]. Unfortunately, most blind watermarking methods embedded multiple copies of the watermark to enhance robustness, which means that these methods can only