Digital Watermarking Based on Neural Network Technology for Grayscale Images

Jeanne Chen
HungKuang University, Taiwan

Tung-Shou Chen
National Taichung Institute of Technology, Taiwan

Keh-Jian Ma
National Taichung Institute of Technology, Taiwan

Pin-Hsin Wang
National Taichung Institute of Technology, Taiwan

BACKGROUND: WATERMARKING

Great advancements made on information and network technologies have brought on much activity on the Internet. Traditional methods of trading and communication are so revolutionized that everything is quasi-online. Amidst the rush to be online emerge the urgent need to protect the massive volumes of data passing through the Internet daily. A highly dependable and secure Internet environment is therefore of utmost importance.

A lot of research has been done in which watermarking has become an important field of research for protecting data. Watermarking is a technique to hide or embed watermark data in a host data (Cox & Miller, 2001; Martin & Kutter, 2001). The embedded watermark could be retrieved at an appropriate time to be used as proof for rightful ownership when one is in question. Both the watermark and the host data could be any media format such as document, still-image, video, audio, and more. The main concentration for this article is on the still-image. The criteria for watermarking technique are imperceptibility and robustness (Cox, Miller, & Bloom, 2000; Hwang, Chang, & Hwang, 2000; Silva & Mayer, 2003). The embedded watermark must not be easily detectable (imperceptible) so as to discourage hacking; once detected, it must not be easy to decrypt. In some instances where hacking are acts with malicious intents—the watermark must withstand (robustness) these attacks and other attacks such as normal image manipulations like sizing, rotations, cropping, and more (Du, Lee, Lee, & Suh, 2002; Lin, Wu, Bloom, Cox, Miller, & Lui, 2001). Robustness here implies that the watermark can still be recovered after suffering attacks of sorts (Miller, Doerr, & Cox, 2004; Niu, Lu, & Sun, 2000; Silva & Mayer, 2003).

The host image can be manipulated for watermark embedding; either in spatial or frequency domain (Gonzalez & Wood, 2002). In spatial domain, an image is perceived as is—but is digitally represented in terms of pixels. Each pixel reflects a spectrum of colors that is perceptible by the human eye system (HVS). In frequency domain, the image is confined to high, medium, and low frequencies with the HVS being less sensitive to high frequency and more sensitive to low frequency. The proposed watermark technique for this article is interested in embedding a watermark in the frequency domain. In the frequency domain, the embedded watermark is less vulnerable to attacks; be it intentional or unintentional. Therefore, the image will be transformed to its frequency domain using the discrete cosine transformation (DCT) (Liu et al., 2002; Hwang et al., 2000).

Furthermore, we are also interested in applying the neural network technology to embed and extract a watermark. By applying the neural network to embed the watermark, we hope to disperse the watermark such that it can be more securely hidden, not easy to decrypt and imperceptible. Neural net-

Copyright © 2005, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

work will again be applied to extract the embedded watermark bits. The train and retrain characteristic could be used to increase the amount of extracted watermark; thereby increasing the chances of getting better quality extracted watermark.

NEURAL NETWORK (NN) TO ENHANCE WATERMARKING

Some of the most popular neural networks (NN) include the Back-propagation Network (BPN), the Probabilistic Neural Network (PNN) and the Counter Propagation Network (CPN). Although the different NNs are devoted to different applications, the basic fundamentals remain in all applications as to how to best apply NN's dynamic learning and error tolerant capacity to get the most accurate results (Davis & Najarian, 2001; Zhang, Wang, & Xiong, 2002). For this article, we are only interested in BPN. BPN is unique for its train and self-train characteristic which can produce more precise trained values. This special characteristic is useful for improving on the watermarking technique such as secure embedment (Hwang et al., 2000) or enhancing the extracted watermark (Tsai, Cheng, & Yu, 2000).

Using NN to Enhance Watermark Embedment

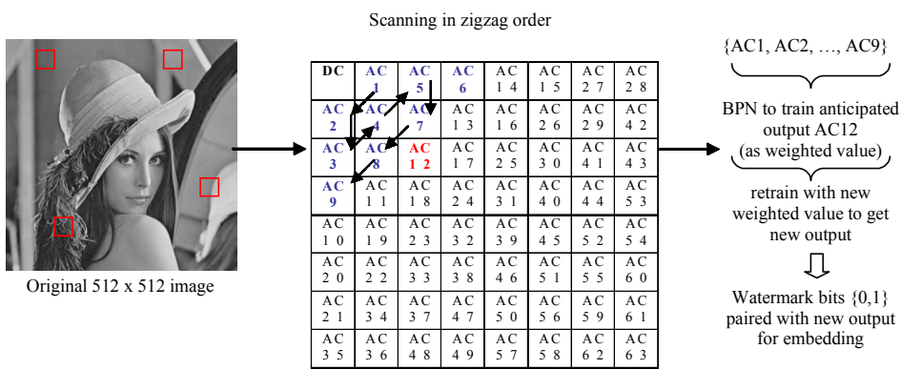
In Hwang et al.'s (2000) method, the watermark will be embedded in the frequency domain. As shown in Figure 1, the host image will first be divided into blocks. These blocks will be individually discrete cosine transformed (DCT) to their frequency domains. The blocks will be scanned in zigzag order to be input as variables to BPN to train for anticipated outputs. Figure 2 shows an example with inputs, {AC1, AC2, …, AC9} with anticipated output {AC12}. The anticipated outputs will be the weighted values used to retrain for a new set of outputs. The final outputs will be paired with the watermark bits {0, 1} to complete the embedding process. Finally, the image will undergo inverse DCT (IDCT) back to spatial domain.

For extraction, the same process will be repeated to divide the image into blocks. Each block will undergo DCT to the frequency domain. The weighted values recorded during BPN training will be used to scan the blocks in zigzag order for the watermark bits. No NN will be applied to the extracted watermark. After watermark had been extracted, the image will be inverse DCT back to spatial domain.

Using NN to enhance the extracted watermark.

In Tsai et al.'s (2000) proposed method the watermark will be first translated into a grouping of 0 and 1 bits. As bits from the grouping are being embedded, they will be tagged. As shown in Figure 3, a 32×32 black and white watermark was embedded into the blue pixels of a 480×512 color host image in spatial domain. The watermark was first converted into bits group *S* which will be randomly encrypted as

Figure 1. Dividing the host image into blocks for DCT



7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/digital-watermarking-based-neural-network/17247

Related Content

Privilege Management Infrastructure
Darren P. Mundyand Oleksandr Otenko (2005). *Encyclopedia of Multimedia Technology and Networking (pp. 849-854).*
www.irma-international.org/chapter/privilege-management-infrastructure/17338

A Novel Strategy for Recommending Multimedia Objects and its Application in the Cultural Heritage Domain
Massimiliano Albanese, Antonio d'Acierno, Vincenzo Moscato, Fabio Persiaand Antonio Picariello (2011). *International Journal of Multimedia Data Engineering and Management (pp. 1-18).*
www.irma-international.org/article/novel-strategy-recommending-multimedia-objects/61309

Mobile Radio Technologies
Christian Kasparand Svenja Hagenhoff (2005). *Encyclopedia of Multimedia Technology and Networking (pp. 645-651).*
www.irma-international.org/chapter/mobile-radio-technologies/17310

A Survey of Information Hiding
M. Hassan Shirali-Shahrezaand Mohammad Shirali-Shahreza (2009). *Handbook of Research on Secure Multimedia Distribution (pp. 241-256).*
www.irma-international.org/chapter/survey-information-hiding/21316

Matching Word-Order Variations and Sorting Results for the iEPG Data Search
Denis Kiselev, Rafal Rzepkaand Kenji Araki (2014). *International Journal of Multimedia Data Engineering and Management (pp. 52-64).*
www.irma-international.org/article/matching-word-order-variations-and-sorting-results-for-the-iepg-data-search/109078