

Chapter 29

Reversible Watermarking in Medical Image Using RDWT and Sub-Sample

Lin Gao

Tianjin Chengjian University, China

Tiegang Gao

Nankai University, China

Jie Zhao

Tianjin Chengjian University, China

ABSTRACT

This paper proposed a reversible medical image watermarking scheme using Redundant Discrete Wavelet Transform (RDWT) and sub-sample. To meet the highly demand of the perceptual quality, the proposed scheme embedding the watermark by modifying the RDWT coefficients. The sub-sample scheme is introduced to the proposed scheme for the enhancement of the embedding capacity. Moreover, to meet the need of security, a PWLCM based image encryption algorithm is introduced for encrypting the image after the watermark embedding. The experimental results suggests that the proposed scheme not only meet the highly demand of the perceptual quality, but also have better embedding capacity than former DWT based scheme. Also the encryption scheme could protect the image contents efficiently.

INTRODUCTION

Digital watermark has been widely used in the copyright protection of digital image. In medical area, reversible watermarking scheme is more preferred than irreversible scheme because of the highly demand on the perceptual quality of the image. Based on the algorithm used to achieve reversible embedding, the reversible watermarking scheme could be categorized into three types: lossless compression based schemes, difference expansion (DE) based schemes and histogram shifting / histogram modifying (HS/HM) based schemes.

DOI: 10.4018/978-1-7998-1763-5.ch029

Reversible Watermarking in Medical Image Using RDWT and Sub-Sample

The lossless compression based schemes first compressed the cover image using lossless compressing scheme(Kountchev, Todorov, Kountcheva, & Milanova, 2006; Maxwell, Handel, & Bradley, 1998; Shih & Wu, 2005). After the compression the size of the cover image has been reduced, the watermark could be embedded into the image by exploit the space generated by the compression. During the extraction process, the watermark was extract from the image, then the compressed image was decompressed using the lossless compression algorithm.

Lossless compression based schemes are easily to achieve. The performance of these schemes is highly depends on the performance of the lossless compression algorithm. The draw back of lossless compression based scheme are robustness and perceptual quality. Because the compressed cover image is vulnerable to the tamper of the stego-image, this kind of scheme usually is not robust against tampering attack. Moreover, since the cover image had been compressed, the visual quality of the stego-image is significantly deduced, which made lossless compression based schemes not suitable for used in medical image watermarking.

Difference expansion based scheme was first proposed by Tian(Tian, 2003) .The main idea of Tian's scheme is as follows: For an 8-bit grayscale image, a pixel pair (x, y) is used to embed a secret bit S, $S \in \{0,1\}$. In the embedding phase, the difference value h and the integer average value l are defined as:

$$h = x - y, l = \left\lfloor \frac{x + y}{2} \right\rfloor \quad (1)$$

The inverse transform is

$$x = l + \left\lfloor \frac{h+1}{2} \right\rfloor, y = l - \left\lfloor \frac{h}{2} \right\rfloor \quad (2)$$

Next, the new difference h' is obtained as follows:

$$h' = 2 \times h + S \quad (3)$$

Finally, the stego-pixel pair (x', y') is obtained by the following transform:

$$x' = l + \left\lfloor \frac{h'+1}{2} \right\rfloor, y' = l - \left\lfloor \frac{h'}{2} \right\rfloor \quad (4)$$

In order to prevent underflow and overflow, the absolute of new difference $|h'|$ after a secret bit S has been embedded must satisfy the following condition:

$$|h'| \leq \min(2 \times (255 - l), 2 \times l + 1) \quad (5)$$

16 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/reversible-watermarking-in-medical-image-using-rdwt-and-sub-sample/244934

Related Content

Secure Key Generation and Management Using Generative Adversarial Networks

Mohammad Al Khaldy, Faisal Aburub, Ahmad Al-Qerem, Amjad Aldweeshand Ammar Almomani (2024). *Innovations in Modern Cryptography* (pp. 165-189).

www.irma-international.org/chapter/secure-key-generation-and-management-using-generative-adversarial-networks/354039

Security, Privacy, and Trust Management and Performance Optimization of Blockchain

Priti Gupta, Abhishek Kumar, Achintya Singhal, Shantanu Saurabhand V. D. Ambeth Kumar (2021). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles* (pp. 134-146).

www.irma-international.org/chapter/security-privacy-and-trust-management-and-performance-optimization-of-blockchain/262699

Authentication of Smart Grid: The Case for Using Merkle Trees

Melesio Calderón Muñozand Melody Moh (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 257-276).

www.irma-international.org/chapter/authentication-of-smart-grid/244918

Decentralizing Privacy Using Blockchain to Protect Private Data and Challenges With IPFS

M. K. Manojand Somayaji Siva Rama Krishnan (2020). *Transforming Businesses With Bitcoin Mining and Blockchain Applications* (pp. 207-220).

www.irma-international.org/chapter/decentralizing-privacy-using-blockchain-to-protect-private-data-and-challenges-with-ipfs/238369

Secure Group Key Agreement Protocols

Kannan Balasubramanianand Mala K. (2018). *Algorithmic Strategies for Solving Complex Problems in Cryptography* (pp. 55-65).

www.irma-international.org/chapter/secure-group-key-agreement-protocols/188512