Watermarking of Digital Images With the Substitution of Low-Value Bits to Increase Capacity

Abdolreza Hatamlou, Department of Computer Science, Khoy Branch, Islamic Azad University, Khoy, Iran
Aliasghar Erfannia, Department of Computer Science, Khoy Branch, Islamic Azad University, Khoy, Iran
Farzaneh Mahalleh, Department of Computer Science, Faculty of Khoy, West Azarbijan Branch, Technical and Vocational University (TVU), Khoy, Iran

ABSTRACT

In this article, a novel watermarking method is proposed which applies the substitution of LSB for low-value parts of the image to embed confidential data. The watermark bits are encoded before being placed. Also, the data on the diameters of the host image blocks are selected on the basis of an irregular determined algorithm that is resistant to attacks. The host image applied in the proposed algorithm should be grayscale. The proposed algorithm uses three bits to embed data that will increase the capacity. In the conventional LSB method, in host image matrix, data are stored in the consecutive numbers, but in this proposed scheme, the host image blocks are divided into separate n x n parts and the diameter of each block are placed in a vector. Then embedded watermarking bits in a vector of numbers is done, from the resulting vector a new block is created, and finally, that block is stored in a new matrix. Then the host image block is overwritten which results in a watermarked image with high capacity.

KEYWORDS

Digital Watermarking, Image Authentication, Reversible Data Embedding, Watermarking Capacity

1. INTRODUCTION

Nowadays, with the rapid development of information technology, digital multimedia data are readily accessible and be distributed. However, this progress causes some problems such as manipulation, illegal copy and distribution of digital data. Digital watermarking provides a solution to this problem (Mintzer et al., 1997) and by putting watermarking signal in digital media to prevent unauthorized use. Watermarking can be classified as invisible watermarking and visible watermarking (Cox et al., 2000; Mintzer et al., 1997). Invisible watermarking is embedding hidden information in a media coverage and its main purpose is security, meaning the inability to prove the existence of the message. However, the visible watermarking is embedding watermarking signal that is visible in the media coverage and it would foreclose possibility of copying and unauthorized use. Three key features for visible watermarking include visibility, clarity and strength of watermarking against possible attacks (Cox et al., 2000; Mintzer et al., 1997).

DOI: 10.4018/IJCVIP.2017100104

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
This paper presents a watermarking method which the image file blocks are divided into separate \( n \times n \) interaction, and the diameter of each block versus other (with no order) are placed in a vector. Then embed watermarking bits in a vector of numbers is done, from the resulting vector, made new block, and finally, block is stored in a new matrix, then the host image block is overwritten.

2. LITERATURE REVIEW

In the visible watermarking, usually transparent watermarked image is produced by adding weight to the edges in an image below watermarking signal is properly preserved. Mintzer et al. (1997) presented a reversible watermarking model image that watermarked image on the host image is visible and the original image can be retrieved. Also, Jung Jin et al. in (2006) presented a visible watermarking method for image authentication that is fully transferable and replaceable. This model is particularly useful for military or medical images. The reversible, visible watermarking method in Yongjian et al. (2006) is a technique based on user key that is applied on visible watermarking signal on human visual system (HVS) to produce visible watermarked image. A user-key method allows authorized users to retrieve high-quality images, while unauthorized users are foreclosed. Shockey et al. in (2006) provided a visible watermarking method using two mapping algorithms: pixel value mapping algorithm (PVMA) and pixel switching algorithm (PPSA). In their method, the pixels are processed by PVMA, and by the PPSA the visible watermarked pixel is formed. By using reverse PPSA and reverse PVMA on watermarked image, the original image is retrieved. In this method for more security random number is added to the watermarking pixels.

Wen-Chao Yang et al. (2008) used the PKI (Public-Key Infrastructure), Public-Key Cryptography and watermark techniques to design a novel testing and verifying method of digital images. The main idea of their paper is to embed encryption watermarks in the least significant bit (LSB) of cover images. Hao Luo et al. (2008), proposed a self-embedding watermarking scheme for digital images. In their proposed algorithm they used the cover image as a watermark. It generates the watermark by halftoning the host image into a halftone image. Then, the watermark is permuted and embedded in the LSB of the host image. The watermark is retrieved from the LSB of the suspicious image and inverse permuted. Saeid Fazli et al. (2009) presented trade-off between imperceptibility and robustness of LSB watermarking using SSIM Quality Metrics. In their algorithm, they put significant bit-planes of the watermark image instead of lower bit-planes of the asset picture. Debjyoti Basu et al. (2010) proposed Bit Plane Index Modulation (BPIM) based fragile watermarking scheme for authenticating RGB color image. By embedding R, G, B component of watermarking image in the R, G, B component of original image, embedding distortion is minimized by adopting least significant bit (LSB) alteration scheme. Their proposed method consists of encoding and decoding methods that can provide public detection capabilities in the absences of original host image and watermark image. Hong Jie He et al. (2006), proposed a wavelet-based fragile watermarking scheme for secure image authentication. In their proposed scheme, they generated the embedded watermark using the discrete wavelet transform (DWT), and then they elaborated security watermark by scrambling encryption is embedded into the least significant bit (LSB) of the host image. Sung-Cheal Byun et al. (2003), proposed a fragile watermarking scheme for authentication of images. They used singular values of singular value decomposition (SVD) of images to check the integrity of images. In order to make authentication data, the singular values are changed to the binary bits using modular arithmetic. Then, they inserted the binary bits into the least significant bits (LSBs) of the original image. The pixels to be changed are randomly selected in the original image. Gil-Je Lee et al. (2008) presented a new LSB digital watermarking scheme by using random mapping function. The idea of their proposed algorithm is embedding watermark randomly in the coordinates of the image by using random function to be more robust than the traditional LSB technique.
Fall Detection Depth-Based Using Tilt Angle and Shape Deformation
www.igi-global.com/article/fall-detection-depth-based-using-tilt-angle-and-shape-deformation/214072?camid=4v1a

Face Match for Family Reunification: Real-World Face Image Retrieval
www.igi-global.com/chapter/face-match-for-family-reunification/196976?camid=4v1a