Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Metadata-based image watermarking for copyright protection

Hsiang-Cheh Huang [a,*], Wai-Chi Fang [b,1]

[a] National University of Kaohsiung, Kaohsiung 811, Taiwan, ROC
[b] National Chiao Tung University, Hsinchu 300, Taiwan, ROC

ARTICLE INFO

Article history:
Available online 17 September 2009

Keywords:
Watermarking
Metadata
Digital rights management (DRM)
Copyright protection

ABSTRACT

In this paper, we propose a practical application for copyright protection of images with watermarking. The EXIF metadata of images and error-control codes are integrated into our algorithm and corresponding applications. Application for robust watermarking is one of the major branches in digital rights management (DRM) systems and digital forensics. Here, we focus on the copyright protection for images taken by ordinary cameras. By use of robust watermarking, it generally alters selected coefficients of the contents to accomplish the embedding process. Should the received image be in question, the watermark embedded beforehand can be extracted to indicate the copyright owner of such an image. We consider not only the image contents itself, but we also employ the EXIF metadata, which serves as the role of watermark, to be integrated into our scheme to make copyright protection possible. Moreover, for enhancing the performance for copyright protection, channel coding is employed and better protection capability can be expected. Taking the manufacturer, camera model, date and time stamp, and other important information in the EXIF metadata into account, conventional watermarking techniques can be applied to ordinary pictures taken by ourselves, and watermarked images with good quality can be produced. Even when the marked image has been intentionally modified, the original EXIF with selected information can mostly be recovered from the channel decoding process. Simulation results present the effectiveness of such an implementation.

1. Introduction

With the fact of the proliferation of consumer electronics devices, most people can easily produce his or her own digital pictures by using digital cameras at any time. As a result, digital images are being accumulated rapidly, and two issues may arise due to this phenomenon. First, how to efficiently arrange and organize pictures is a major task for the picture owners. And next, the copyrights of these pictures should be retained to prevent from the illegal use by other people. Thus, automated tools for organizing these pictures have become a necessity for users, and we aim at taking advantage of the information relating to the automatic tools to make copyright protection possible. With the large amount of pictures captured, in order to ease the task for organizing and classifying the vast amount of digital pictures, the EXchangeable Image File format (EXIF) is proposed to help store important information into the header of digital image files, including the date and time information, the settings of the camera, and the resolutions of the picture. In addition to the main purpose of EXIF for helping users to organize and classify the pictures taken, we can also apply the EXIF to the scope of digital forensics area to conquer the tampering problem, which are frequently encountered due to the ease of editing the digital images. Therefore, we focus on watermarking with EXIF in this paper.

* Corresponding author. Tel.: +886 918 952 075; fax: +886 7 591 9374.
E-mail addresses: huang.hc@gmail.com (H.-C. Huang), wfang@mail.nctu.edu.tw (W.-C. Fang).
URLs: http://hchuang.ee.nuk.edu.tw/ (H.-C. Huang), http://soc.nctu.edu.tw (W.-C. Fang).

[1] IEEE Fellow, TSMC Distinguished Chair Professor, National Chiao Tung University.

1569-190X/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.simpat.2009.09.004

Here, we use the digital images, taken by different cameras, to perform the applicability of watermarking with the aid of EXIF. It is generally agreed that for watermarking algorithms, the watermarked image quality (or imperceptibility), the survivability after intentional attacks (or robustness), and the number of bits embedded (or capacity) are the three most important factors to assess how good the algorithm and the implementation are. Hence, we integrate our algorithm with discrete cosine transform (DCT), choose the reasonable amount of information in EXIF metadata, and select the appropriate DCT coefficients for watermark embedding. To enhance the robustness of the extracted EXIF metadata, the BCH (Bose–Chaudhuri–Hocquenghem) codes are used, and better results can be expected due to its error-correcting capability. Experiments are conducted under the scenario that when the watermarked images are attacked by some means, the selected information in EXIF can be recovered back to some extent, and then the copyrights of such images can be protected.

This paper is organized as follows. Section 2 depicts the scheme for watermark generation with the aid of EXIF metadata. Section 3 describes the watermarking scheme proposed in this paper. Experimental results are presented in Section 4. Finally, Section 5 gives the conclusion of this paper.

2. Watermarking with EXIF

2.1. Description of EXIF metadata

EXIF is a standard for the JPEG- and TIFF-image formats, mainly used by digital cameras [1–3]. It contains information about camera settings and shooting environment of the camera and the picture itself [4], including the date and time that the picture is taken, the camera manufacturer and camera model, the horizontal and vertical resolutions of the picture, shutter speed, ISO speed, white balance, flash utilization, etc. The copyright and geographic information can also be included [5,6]. The major purpose for EXIF metadata is to offer the utility for accurate searching, retrieval, and viewing [7,8]. Unfortunately, they are usually not completely recorded and supported due to different implementations and incomplete support of early digital cameras. The major purpose of this paper is to take the EXIF metadata into consideration in order to make copyright protection possible. Therefore, for using the metadata to serve as the watermark, the necessary portion should be carefully chosen to meet the scope that selected information can be interpreted by most cameras. Fig. 1a is an example for the pictures taken by ourselves, and Fig. 1b is the associated EXIF metadata extracted by our program. Fig. 2 shows the example by using another camera with a different brand. Taking EXIF utilities into account, we extend its scope from effective organization and retrieval of images to the application of copyright protection and tamper resistance.

As we stated in Section 1, three requirements considered mostly are imperceptibility, robustness, and capacity. Taking practical implementations into account, we convert the EXIF metadata into bitstreams by using their ASCII representations, and choose to embed at most 1 bit per 8×8 block in the middle-frequency coefficients with different embedding strengths.

2.2. Generation of watermark information with EXIF metadata

In this paper, we use the ordinary pictures taken by ourselves by using ordinary cameras, illustrated in Figs. 1a and 2a, respectively, and they both have the sizes of 2048×1536. Hence, considering the purposes for implementation, our algorithm can be integrated into the DCT-based transform coding and the associated JPEG compression schemes. With the assumption that at most 1 bit can be hidden into one block with the size of 8×8, we are able to embed the watermark with the maximal capacity of $\frac{2048}{8} \times \frac{1536}{8} = 49152$ bits. We choose the watermark information, including

- the camera model and the vendor data,
- the time and date stamps, and
- picture resolutions,

in EXIF metadata. Information selected for both pictures are shown in Figs. 1b and 2b for more details, which make a total of 171 and 238 bytes, respectively. Since all the characters are represented by ASCII codes, we take the binary form of the information, 1368 and 1904 bits in total, to serve as the watermark information. Since we are going to verify the applicability of our algorithm and 49,152 bits can be embedded at most, we choose a much fewer capacity and leave the remaining capacity for the insertion of other necessary data at later times. In order to enhance the capability for copyright protection and the robustness against attacks, unlike previous approaches to repeat the same watermark information for several times [10,11], channel coding can be utilized for enhanced robustness [12]. The total capacity for repeated watermark is much larger than that of the BCH-coded watermark depending on how many times the data is repeated. Since more embedded capacity leads to more degradation of the watermarked image, we choose to use the error-control codes, which only generate a portion of redundancy compared to the repeated case, for better protection of embedded information. We use BCH codes [13] with different error-correcting capabilities to encode the watermark information, and to generate the embedded bitstream. And then we can see how BCH codes help to improve the performance of the extracted watermark.

The BCH (Bose–Chaudhuri–Hocquenghem) codes form a large class of multiple random error-correcting codes. For any integer $m \geqslant 3$ and $t < 2^{m-1}$, there exists a primitive BCH code with the following parameters: