Copyright Protection for Images with EXIF Metadata

Hsiang-Cheh Huang [A], Yueh-Hong Chen [B], Shin-Chang Chen [A]

[A] *National University of Kaohsiung, Taiwan, R.O.C.*
hch.nuk@gmail.com

[B] *National Chiao Tung University, Taiwan, R.O.C.*
yuehhong@gmail.com

[A] *National University of Kaohsiung, Taiwan, R.O.C.*
m0965115@mail.nuk.edu.tw

Abstract

In this paper, we propose an application of robust watermarking with the aid of EXIF metadata in digital images. Application for robust watermarking is one of the major branches in digital rights management (DRM) systems. Furthermore, implementation schemes for robust watermarking generally alter selected pixels in the spatial domain, or corresponding coefficients in the transform domain, to accomplish the embedding process. We consider not only the pixels or coefficients in the images, but we also employ the EXIF metadata, which serves as the role of watermark, to further protect the copyrights. Taking the manufacturer, camera model, date and time stamp, and some other information in the EXIF metadata as the watermark information, 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 be recovered from the watermark extraction process. Simulation results present the effectiveness of such an implementation.

1. Introduction

Nowadays, due to 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 automated tools for organizing these pictures have become a necessity for users. With the large amount of pictures captured, the EXchangeable Image File format (EXIF) is used to help store some information about the digital camera, including the date and time information, the settings of the camera, and the copyright information. In addition to the main purpose of EXIF for helping users to organize and classify the pictures taken, we can apply the EXIF to the scope of digital forensics area to conquer the tampering problem that are frequently encountered due to the ease of editing the digital files. Therefore, we focus on watermarking and its application in DRM in this paper.

In this paper, we use the digital images, taken by different cameras, to represent the multimedia contents for copyright protection. It is generally agreed that for one watermarking algorithm, 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 implementation are. Hence, we implement 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. 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 hence the copyrights of such images can be protected.

This paper is organized as follows. In Section 2 we briefly describe the composition of EXIF, and the necessary information that we choose. In Section 3 we present the proposed algorithm for watermark embedding and extraction with DCT. Simulation results are demonstrated in Section 4. Finally, we conclude this paper in Section 5.

2. EXIF Information for Watermarking

2.1 Composition of EXIF metadata

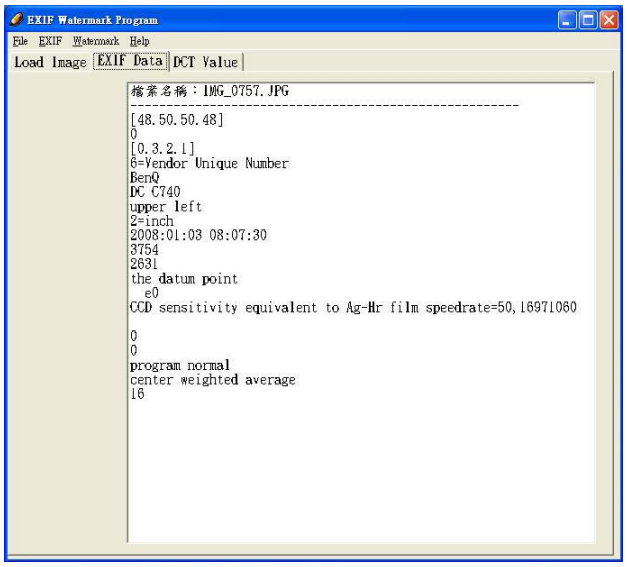
EXIF is a specification for the JPEG and TIFF image file formats, mainly used by digital cameras [1][2][3][4]. It contains information about camera settings and shooting environment of the camera and the picture itself, including the date and time that the picture is taken, the camera manufacturer and the camera model to take the picture, the horizontal and vertical resolutions of the picture, the shutter speed, ISO speed, and the aperture for the camera settings, white balance, subject distance and flash utilization, etc. The copyright information and the geographic information that the picture is taken can also be included in the EXIF [5][6]. Unfortunately, EXIF metadata are usually not completely recorded due to different implementations and incomplete support of early

978-0-7695-3278-3/08 $25.00 © 2008 IEEE
DOI 10.1109/IIH-MSP.2008.167

IEEE computer society

digital cameras. Therefore, for employing the metadata to serve as the watermark, parameters need to be carefully chosen. Figure 1(a) is an example for the picture taken by ourselves, and Figure 1(b) is the associated EXIF metadata extracted by our program.

(a)



(b)

Figure 1. (a) Original image in this paper. (b) Selected information of EXIF.

The major purpose for EXIF metadata is to help people to efficiently arrange and organize the vast amount of images. For instance, for a digital camera that has resolution of 6 megapixels, compressed by JPEG, and is equipped with a 2GB storage device, it would generally produce more than 700 pictures when running out of memory. After moving the 700 pictures to the PC, the 2GB memory device is cleared, and another 700 pictures can be produced subsequently, and this process can be repeated again and again. Thus, how to effectively and efficiently organize and search for the 700, or virtually unlimited amount of digital images, is a problem for most people, and EXIF metadata offer the utility for accurate searching, retrieval, and viewing purposes [7][8][9][10].

As we stated in Sec. 1 and in previous works, even though lots of parameters can be taken into account for designing a robust watermarking system, three most commonly considered requirements are imperceptibility, robustness, and capacity. Namely, the watermarked image quality should be good, the extracted watermark should be meaningful, and the amount of capacity should be reasonable. Taking practical implementations into account, we transform the EXIF metadata into bitstreams, and choose to embed 1 bit per 8×8 block in the middle frequency coefficients with different embedding strengths.

2.2 The watermark data

Because there is much information contained in EXIF metadata, the necessary portion should be carefully chosen to serve as the watermark information [11][12].

In this paper, we use the ordinary picture taken by ourselves, illustrated in Figure 1(a), with the size of 2048×1536. Hence, we are able to embed $\frac{2048}{8} \times \frac{1536}{8} = 49152$ bits. We choose the information including camera model and vendor, time stamp, and other settings shown in Figure 1(b), which makes a total of 238 bytes. Since all the characters are represented by ASCII codes, we take the binary form of the information, 1904 bits in total, to serve as the embedded bitstream. In order to enhance the robustness against attacks, we repeat the bitstream for 19 times to represent the watermark. By doing so, the watermark has 36176 bits, which is below the maximum number of allowable capacity. Also, fewer bits embedded means less alteration to the original image, and it leads to better watermarked image quality subjectively.

3. Proposed Algorithm

We follow conventional DCT-based watermarking techniques with some necessary modifications for integrating with the EXIF metadata. Steps are depicted as follows.

3.1 Deciding the necessary information

We plan to embed at most 1 bit per 8×8 block. Since the resolutions of images differ from one camera to another, the capacity of the necessary information needs to be carefully chosen to be within the practical range. We choose the commonly seen parameters, shown in Figure 1(b), and use the ASCII representation of these parameters to serve as the binary watermark.

3.2 Embedding watermark with DCT

We modify some conventional scheme [13][14] for DCT-based watermarking to embed the binary watermark.

Step 1. *Performing the DCT of original image*: 8×8 DCT is performed on the entire 2048×1536 image. Since the original image is color image, we embed the watermark into the red plane. In one block, it leads to one DC coefficient, presented by position 0, and 63 AC coefficients, presented by positions 1 to 63.

Step 2. *Determining the position for embedding:* It is suggested to embed the watermark into middle frequency coefficients [14] to meet the watermarking requirements. Therefore, we choose to embed our watermark into the AC11 coefficient of every block.

Step 3. *Obtaining the threshold for embedding:* The ratio between the average value of DC and AC11 coefficients among the $\frac{2048}{8} \times \frac{1536}{8} = 49152$ blocks is served as the threshold for watermark embedding.

Step 4. *Embedding the watermark bits:* By taking the threshold in Step 3, it will meet one of the two situations below.

- If bit 0 is embedded, and if the original AC11 is larger than the threshold value, it is decreased to be smaller than the threshold by a parameter δ, called the embedding strength. If not, keep the value unchanged.
- If bit 1 is embedded, and if the original AC11 is larger than the threshold value, keep the value unchanged. If not, it is increased to be larger than the threshold by δ.

Step 5. *Performing the inverse DCT of modified coefficients:* Inverse DCT is calculated to obtain the watermarked image. We use the peak signal-to-noise ratio (PSNR) to evaluate the watermarked image quality.

3.3 Choosing proper attacks

For verifying watermarking algorithm, applying attacks to watermarked image is necessary. We choose JPEG compression, low-pass filtering (LPF), and median filtering (MF), to perform the attacks. To assess the robustness, the bit-correct rate (BCR) and symbol-correct rate (SCR) values after experiencing these attacks are calculated. Here, the BCR is the percentage of the number of correctly extracted bits, and the SCR is that of the correctly decoded ASCII symbol in EXIF metadata. The higher the two values, the better the outcomes.

3.4 Extraction of watermark and decoding of Metadata

Watermark bits can be extracted based on the threshold in Step 3 in Sec. 3.2. The BCR of these bits can be calculated. Next, since the extracted bits are the concatenation of ASCII symbols for 19 times, we use majority vote to determine the binary representation of symbols, and then the decoded symbols can be obtained. The SCR can now be calculated.

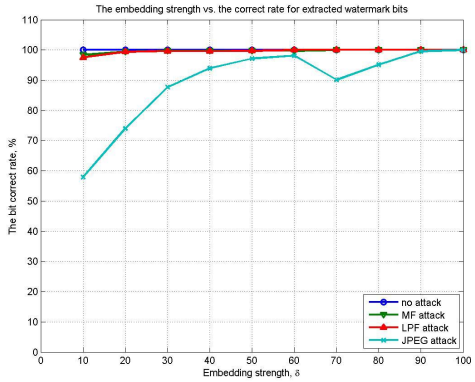
4. Experimental Results

We choose the ordinary picture in Figure 1(a), the selected EXIF information in Figure 1(b), and perform watermark embedding with the embedding strength of δ=50 into the AC11 coefficients in the DCT domain. The watermarked image is illustrated in Figure 2, with the PSNR of 46.33 dB.

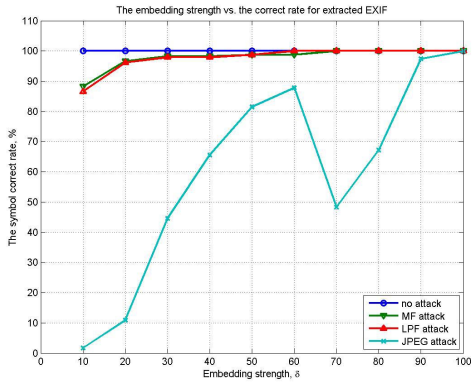
Figure 2. The watermarked image with PSNR = 46.33 dB.

We also apply three commonly employed attacks, namely, JPEG, LPF, and MF attacks, in addition to the no attack case, for verifying the robustness in the binary watermark and the corresponding EXIF metadata. By changing the embedding strengths from δ=10 to δ=100, we present the extracted BCR in Figure 3(a), and that of the SCR in Figure 3(b), respectively. In Figure 3(a), for the no attack, LPF attack, and MF attack cases, the BCR gets increased with the increase of embedding strength. Result with JPEG attack has comparable performance to the other three cases when we use larger embedding strengths. And in Figure 3(b), we can see that comparing to Figure 3(a), the corresponding SCR values seem degraded. It is reasonable because a symbol can be correctly decoded when all the binary composition in ASCII need to be correctly extracted. If one bit in one symbol is extracted erroneously,

we still have high BCR but the symbol cannot be correctly decoded.



(a)



(b)

Figure 3. Correct rates for extracted data under different embedding strengths. (a) The bit correct rate. (b) The symbol correct rate.

Summing up, when we embed the EXIF metadata with reasonable capacity into the middle frequency coefficients in the DCT domain, acceptable image quality and robustness can be reached.

5. Conclusion

In this paper, we discussed about the practical implementation of robust watermarking with EXIF metadata. By finding the necessary information in EXIF, it can be served as binary watermark for embedding. Simulation results depict that the metadata can be perfectly extracted with increased embedding strengths, and our algorithm is robust to common attacks. By using channel coding to protect the selected metadata can be further exploited in the future.

6. References

[1] Standard of Japan Electronics and Information Technology Industries Association, JEITA CP-3451, *Exchangeable image file format for digital still cameras : Exif Version 2.2*, http://www.jeita.or.jp/english/standard/html/1_4.htm, 2002.

[2] X. Liu, L. Zhang, M. Li, H. Zhang, and D. Wang, ``Boosting image classification with LDA-based feature combination for digital photograph management,'' *Pattern Recognition*, vol. 38, no. 6, pp. 887-901, June, 2005.

[3] J. Tesic, ``Metadata practices for consumer photos,'' *IEEE Multimedia*, vol. 12, no. 3, pp. 86-92, Jul.-Sep. 2005.

[4] B. K. Smith, J. Frost, M. Albayrak and R. Sudhakar, ``Integrating glucometers and digital photography as experience capture tools to enhance patient understanding and communication of diabetes self-management practices,'' *Personal and Ubiquitous Computing*, vol. 11, no. 4, pp. 273-286, Apr. 2007.

[5] N. Sinha, ``Secure embedded data schemes for user adaptive multimedia presentation,'' *Journal of Digital Information*, vol. 6, no. 4, 2005.

[6] W. Luo, Z. Qu, F. Pan, and J. Huang, ``A survey of passive technology for digital image forensics,'' *Frontiers of Computer Science in China*, vol. 1, no. 2, pp. 166-179, May 2007.

[7] C.-J. Jang, J.-Y. Lee, J.-W. Lee, and H.-G. Cho, ``Smart management system for digital photographs using temporal and spatial features with EXIF metadata,'' *2nd Int'l Conf. on Digital Information Management*, vol. 1, pp. 110-115, 2007.

[8] M. Boutell and J. Luo, ``Photo classification by integrating image content and camera metadata,'' *Int'l Conf. on Pattern Recognition*, vol. 4, pp. 901-904, 2004.

[9] I. Arai, K. Fujikawa, and H. Sunahara, ``Proposal of time-crawler which collects an event time by reading EXIF data in blogs,'' *2008 Annual IEEE Student Paper Conference*, pp. 1-4, 2008.

[10] S. Sarin, T. Nagahashi, T. Miyosawa, and W. Kameyama, ``On automatic contextual metadata generation for personal digital photographs,'' *The 9th Int'l Conf. on Advanced Communication Technology*, vol. 1, pp. 66-71, 2007.

[11] J. S. Pan, H.-C. Huang, and L. C. Jain (editors), *Intelligent Watermarking Techniques*, World Scientific Publishing Company, Singapore, Feb. 2004.

[12] J. S. Pan, H.-C. Huang, L. C. Jain, and W. C. Fang (editors), *Intelligent Multimedia Data Hiding*, Springer, Berlin-Heidelberg, Germany, Apr. 2007.

[13] C. S. Shieh, H.-C. Huang, F. H. Wang, J. S. Pan, ``Genetic watermarking based on transform domain techniques,'' *Patt. Recog.*, vol. 37, no. 3, pp. 555--565, Mar. 2004.

[14] S. C. Chu, H.-C. Huang, Y. Shi, S. Y. Wu, and C. S. Shieh, ``Genetic Watermarking for Zerotree-Based Applications,'' *Circuits, Systems, and Signal Processing*, vol. 27, no. 2, pp. 171--182, Apr. 2008.