MVA2007 IAPR Conference on Machine Vision Applications, May 16-18, 2007, Tokyo, JAPAN

An effective watermark embedding algorithm for high JPEG compression

Hui-Yu Huang
Department of Computer Science and Information Engineering, National Formosa University, Taiwan
E-mail: hyhuang@nfu.edu.tw

Chi-Hung Fan, and Wen-Hsing Hsu
Department of Electrical Engineering, National Tsing Hua University, Taiwan

Abstract

Digital watermarking is an important technology that has been widely applied many applications. In this paper, we present an effective embedding watermark method for JPEG image which can resist high compression attack and retain a good image quality. The proposed algorithm consists of three parts which are searching the optimal embedded position, embedded value, and embedded/extracted processing for watermark in images. First, the embedded position search, which performed in DCT domain, are achieved the optimal watermark embedding position by means of finding the number of zero in low frequency region after compressing. Next, according to above result, we calculate the distortion difference between the original image and compressed image to decide the best tolerant range and assign the embedded value. Last, based on quantization index modulation (QIM), the embedded processing can further achieve effectively to inset the watermark in images. Thus this approach can effectively resist high JPEG compression and protect the embedded information and media ownership. The experimental results are presented to demonstrate the effectiveness of our approach.

1. Introduce

Owing to the quickly evolvement of networked multi media systems in last few years, the protection of digital media has been necessitated and more important scheme, especially the protection and enforcement of intellectual property rights. Copyright protection involves the authentication of data (text/image/video) ownership and the identification of illegal behavior such as copies. Techniques are needed to prevent the copying, forgery and unauthorized distribution of images and video. However, digital watermarking technology is usually applied to protect the intellectual property of digital data which are freely available on the WWW and transmitted over network.

A large number of watermarking systems address the problems of implementing invisible watermarks. There have been a number of corresponding works [1-3] dedicated to image/video/audio watermarking. These scholars define a digital watermark as an identification code which carrying information about the copyright owner, the creator of the work, the authorized consumer, etc. It is permanently embedded into digital data for copyright protection and may be used for checking whether the data have been modified illegally [1]. Cox *et al*. [3] proposed a secure (tamper-resistant) algorithm to construct the watermark as an independent and identically distributed Gaussian random vector which is inserted in a spread-spectrum-like fashion into spectral component of the data. It can effectively resisted against the transformed watermarked image. Owing to the time-consuming computation for spread-spectrum method, Chen [4] proposed the quantization index modulation (QIM) and distortion-compensated (DC-QIM) methods to embed the watermark in order to improve this program. By using of the (QIM) algorithm, it can achieve against arbitrary bounded and fully informed attacks and further arise to currently popular spread-spectrum method. Wong [5] used the human visual system (HVS) model to estimate the JEPG-to-JEPG data hiding capacity of JPEG image and the maximum number of bits embedded in JPEG-compressed images. Wong *et al.* [6] proposed three techniques which include single watermark embedding, multiple watermark embedding, and iterative watermark embedding to embedded watermarks in order to remain good image quality and robust in varying degree to JPEG compression. This algorithm can successively embedded watermark when the quality factor is low, but when the quality factor is low. However, this approach makes high computation complexity of the iterative loop. These methods are also existed the problems of either complexity or time-consuming computation.

Generally, the watermark scheme hopes the abilities of resisting some attacks such as noise, copying, rotation, scaling, lossy compression, etc. However, we find out that many researches do not have an effective method to solve this problem well. Although, a lot of watermarking systems designed for compression have been proposed, most of them may not make a balance point between image quality and compression intensity. Therefore, we design an optimal method in order to solve this problem between image quality and compression intensity. In this paper, our proposed system will concern with resisting high lossy compression for JPEG to protect the intellectual property rights of owner against the illegal infringement.

The rest of this paper is organized as follows. Section 2 distributes the proposed method. In Section 3, we will present the experimental results. Finally, Section 4 gives the brief conclusions.

2. Proposed Method

The proposed method consists of three stages. First, in order to protect the watermarking under JPEG compression, we present an analysis method to find out the best embedded value for every input image. In this analysis method, we can find out the best tolerant range which can resist the general JPEG compression ratio. Second, in order to resist high JPEG compression, we present a technique to find the best embedded points for image, which has the best resistant ability of high JPEG compression processing. After performing the first and second items, we can obtain the information of embedded watermark. Third, using the previous results which the information of the embedded points and embedded values from an input image, we will insert the watermark into the host image. Based on QIM (Quantization Index Modulation) [4-6], we will further improve the performance of the QIM algorithm to construct our embedded processing.

The flowchart of our proposed system is illustrated in Figure 1. The system consists of the embedded positions search, embedded values search, and embedded and extracted processing. In addition, in order to achieve the system robustness, we adopt a secure key to restore the embedded information which will be used in the embedded and extracted processing. In the following subsections, we will describe the algorithm in detail.

2.1 Embedded points search

It is well-known JPEG compression that will lead to distortion information of the host image. Generally, there are two kinds of situations to affect the extracting processing under JPEG compression. One is the host image has been compressed, it will cause the host image distortion. The other is the compression ratio has been exceedingly limited; it will cause the original data to be zero in the DCT domain. Hence, we define a variable $ZNum(x, y)$ to represent the total numbers of this situation as zero coefficient corresponding to the coordinates (x, y). If this situation happened, it may loss the embedded information that stores the watermark data. Therefore, we design the optimal embedded positions/points searching algorithm in order to solve above problems. The mean of optimal embedded points is that all of points have more resistive ability of JPEG compression than other points in each block.

It is important step that can help to achieve high performance against JPEG compression. Next, this searching step is described as follows.

Step1: Using JPEG Compression which QFactor from 1 to 100 to compress $Q_i(x, y)$ corresponding the coordinates (x, y).

Step2: Translating the images to DCT domain by every 8×8 block.

Step3: Calculating the compressive zero numbers ($ZNum(x, y)$) in every point.

Step4: Searching the low frequency positions not including DC for each 8×8 block can find out the optimal embedded points which have the minimum compressive zero numbers. (If our image size is 720×480, then we have 90×60 numbers of optimal embedded points.)

Step5: Saving the information to these points in a secure key.

2.2 Embedded values assignment

The other situation to affect the extracting process under JPEG compression is that any compression ratio will cause distortion of the host image. It is common and important problem that needs us to solve more serious. Because an unsuitable embedded value may cause a fail extracting data under JPEG compression.

Hence, based on above steps, it is known that every block possesses corresponding to the optimal embedded point. Each of the optimal embedded points may have a chance to adopt in embedded watermark point. Therefore, in order to resist JPEG compression, calculating the optimal embedded value in each optimal embedded point is needed. In this subsection, we will further find out the best tolerant range that can resist the great part of JPEG compression ratios. Next, the optimal embedded values assignment is described in the following.

Step1: Using JPEG Compression which QFactor from 1 to 100 to compress host image ($Q_i(x, y)$).

Step2: Translating the images to DCT domain by every 8×8 block.

Step3: Calculating the distortion between original image and compressive image in DCT domain. If the reconstructed value is bigger than original value, we call it a positive distortion. If the reconstructed value is smaller than original value, we call it a negative distortion. Then the maximum positive distortion ($MPD(i)$) and maximum negative distortion ($MND(i)$) will be found.

Step4: Determining the maximum distortion range ($MDR(i)$) is the best tolerant range for embedded point, and defined as

$$MDR(i) = \max(MPD(i), MND(i)). \quad (1)$$

Step5: Saving the information of the range in a secure key.

2.3 Embedded and extracted processing

2.3.1 Embedded processing

In order to obtain the optimal positions to embed watermark, we have to further find out the embedded watermarking positions $EWP(m,n)$ and values $EWV(m,n)$ corresponding the coordinates (m,n) of watermark. According to above processing, all of the optimal embedded points $OEP(p,q)$ can be found which can tolerant higher JPEG compression ratio corresponding to the *pth* row and *qth* column of block location and have the relatively number of zero coefficient by compression processing. Now we use this information to decide the $EWP(m,n)$. The searching rule is that the number of zero coefficient for $EWP(m,n)$ must be greater than a threshold value and the searching path is started at the threshold to 100. In our experiment, this threshold is set to 30, namely, searching the $EWP(m,n)$ position is started from 30 to 100. While the number of $EWP(m,n)$ are equal to the number of embedded watermark, the searching process is stopped. Every $EWP(m,n)$ has the corresponding $EWV(m,n)$ value that can easy to obtain by means of the optimal embedded value $OEP(p,q)$. Here, our system will not search $EWP(m,n)$ from 0 to 100, it is because that if the threshold is set to 0, it will cause the serious distortion of watermark image. Actually, it is a reasonable situation; a point which is the low number of zero coefficient can serve as a sensitive point under JPEG compression.

Figure 2 is shown in the embedded method based on improved quantization index modulation mechanism. All of the embedded procedures will be distributed as follows.

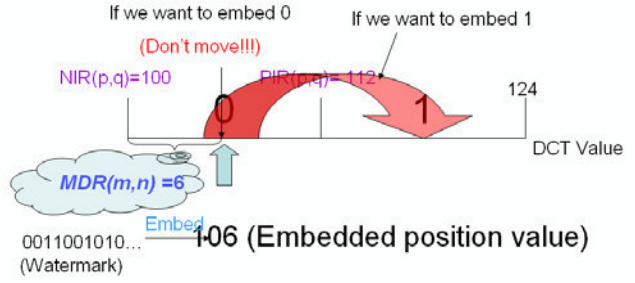

Figure 2 The diagram of the proposed embedded method.

Step1: Load the information of $EWP(m,n)$ to know where is the embedded point and also read-out its original host image DCT value ($Q_i(x,y)$) in this point.

Step2: Find out the positive index range $PIR(i)$ and negative index range $NIR(i)$ for the *ith* point that will be used to extracted process and this information serves as secure key.

$$IR(I)=\begin{cases} NIR(i)=Oi(x,y)-MDR(i), \\ PIR(i)=Oi(x,y)+MDR(i), \end{cases} \quad (2)$$

where $Q_i(x,y)$ is the DCT value of the original host image corresponding to the embedded point.

Step3: Define the index range (*IR*).

$$IR(i)=\begin{cases} 0, \ where \ NIR(i)\le W_i(x,y)\le PIR(i), \\ 1, \ where \ NIR(i)\ge W_i(x,y) \ or \ PIR(i)\le W_i(x,y), \end{cases} \quad (3)$$

where $W_i(x,y)$ is the DCT value of embedded point for watermark image.

Step4: Insert the watermark in the host image.

$$W_i(x,y)=\begin{cases} O_i(x,y)+2\times EWV(i), & \text{if embed } 1, \\ O_i(x,y), & \text{if embed } 0, \end{cases} \quad (4)$$

If we want to embed index (=0), we don't need to change its value. If we want to embed index (=1), we need to move the original DCT value out of the index range.

Step5: Repeat ***step1*** to ***step4*** until all of the watermarks are embedded.

2.3.2 Extracted processing

In extracted method, we must make use of the secure key obtained by the embedded process which is denoted the negative index range $NIR(i)$ and positive index range $PIR(i)$ information. By above the information, then it is easy to detect the embedded watermark. And its procedure is expressed by

$$IR(i)=\begin{cases} 0, \ if \ NIR(i)\le W_i(x,y)\le PIR(i), \\ 1, \ if \ NIR(i)\ge W_i(x,y) \ or \ PIR(i)\le W_i(x,y), \end{cases} \quad (5)$$

where $W_i(x,y)$ is the DCT value of embedded point of the watermark image.

3. Experimental Results and Discussion

In this section, we show some experimental results by our proposed algorithm. Here we use the size 720×480 of Mandrill standard image to be our host image and the 30×20 size of the watermark shown in Figure 3. A similarity measurement (*NC*) of the extracted and the referenced watermarks is defined as:

$$NC=\frac{\sum_{i=0}^{m}\sum_{j=0}^{n} w(i,j)\hat{w}(i,j)}{\sum_{i=0}^{m}\sum_{j=0}^{n}[w(i,j)]^2}, \quad (5)$$

where $w(i,j)$ and $\hat{w}(i,j)$ denote the original watermark and the extracted watermark corresponding to the coordinates (i,j) respectively.

Figure 4 shows the *NC* value in the different QFactor value. From the Figure 4, it is obvious that the *NC* value can

keep up 0.975 when the QFactor value is decreased. The *NC* results compared with Hsu [7] and Wu *et al.* [8] for the different compression ratio is shown in Figure 5. It is shown that our proposed method can effectively resist the high compression ratio. According to above experimental results by means of our process method, the embedded position and embedded value can effectively find out and assign within DCT domain.

(a) (b) PSNR = 44.6562dB

(c)

Figure 3 (a) Host image, (b) embedded watermark image, and (c) the watermark.

(a) QFactor = 90, *NC* = 1.0000.

(b) QFactor = 70, *NC* = 0.9900.

(c) QFactor = 50, *NC* = 0.9933.

(d) QFactor = 30, *NC* = 0.9888.

Figure 4 Extracted watermarks in different QFactor.

The maximum distortion range to embedded point can be found. On the other hand, based on QIM technique and the design of maximum distortion range, we can robustly embed the watermark into the image. Consequently, our approach is possessed a robust ability to resist high compression ratio attacks and further to protect the intellectual property rights.

4. Conclusions

Based on protecting the copyright of digital media data, we propose a robust digital watermarking technique to effectively embed the watermark in high JPEG compression. It is primarily find the optimal embedded positions to embed the watermark in high JPEG compression.

It is primarily find the optimal embedded positions to embed the watermark in high JPEG compression. Consequently, according to above results, it is shown that our approach can effectively improve the robustness for digital watermarking against JPEG compression to achieve the copyright announce. For the compression attacks, it is found that the robustness against JPEG compression is achieved for a compression ratio up to 30.

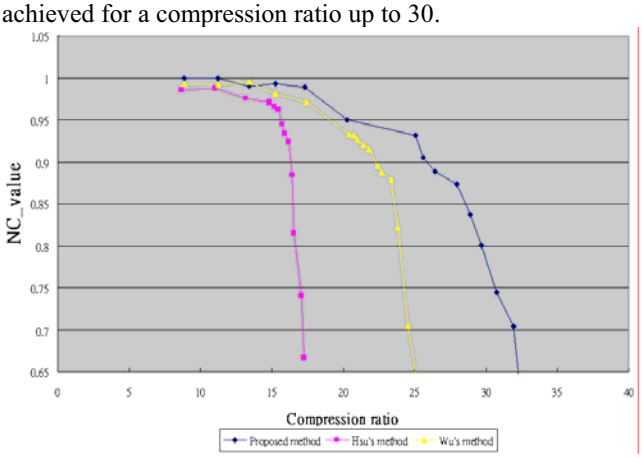

Figure 5 The *NC* results of the different compression ratio.

Acknowledgments. This work was supported in part by the National Science Council of Republic of China under Grant No. NSC94-2213-E-007-075.

References

[1] W. Funk, C. Busch and S. Wolthusen, "Digital watermarking: From concepts to real-time video applications," *IEEE Comput. Graphics Applicat*., Vol. 19, pp. 25-35, 1999.

[2] M. Kobayshi, M. D. Swanson, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proc. IEEE*, Vol. 86, pp. 1064-1087, 1998.

[3] F. T. Leighton, I. Cox, J. Kilian, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, Vol. 6, pp. 1673-1687, 1997.

[4] B. Chen, and G. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory*, Vol. 47, pp. 1423-1443, 2001.

[5] A. Chang, P. H. W. Wong, and O. C. Au, "On improving the iterative watermark embedding technique for jpeg-to-jpeg watermarking," in *Proc. of Int. Symposium on Circuits and Systems (ISCAS'04)*, Vol. 2, pp. 161-164, 2004.

[6] P. H. W. Wong, and O. C. Au, "A capacity estimation technique for jpeg-to-jpeg image watermarking," *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 13, pp. 746-752, 2003.

[7] C. T. Hsu, and J. L. Wu, "Hidden digital watermarks in images," *IEEE Trans. on Image Processing*, Vol. 8, Issue 1, pp. 58-68, 1999.

[8] G. Z. Wu, Y. J. Wang, and W. H. Hsu, "Robust watermark embedding/detection algorithm for H.264 video," *Journal of Electronic Imaging*, Vol. 14, No. 1, pp. 1-9, 2005