Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **1**, January **2015**

A Robust Blind Image Watermarking Scheme Based on Classified Vector Quantization

Xu Ding, Zhe-Ming Lu* and Fa-Xin Yu
School of Aeronautics and Astronautics
Zhejiang University
Hangzhou, 310027, P. R. China
zheminglu@zju.edu.cn

Ting-Yuan Nie and Jie Sun
School of Science
Qingdao Technological University
Qingdao, 266033, P. R. China
tynie@qtech.edu.cn; sj1979419@163.com

Received May 2014; revised July 2014
(Communicated by Zhe-Ming Lu)

Abstract. *Since 2000, many digital watermarking schemes for vector quantization (VQ)-compressed images have been proposed. Their main idea is to carry watermark information by VQ codeword indices. The advantage of this kind of watermarking schemes is its robustness to VQ compression with the same codebook. This Letter presents a more effective image watermarking method based on classified VQ. First, the input image is segmented into blocks and a classifier is used to classify each block. Then, each block is encoded by the classified VQ codebook according to its class and the two watermark bits corresponding codebook. Experimental results show that the proposed scheme is a blind watermarking method which outperforms existing VQ-based watermarking methods, and the watermarked image is robust to most of common signal processing operations.*
Keywords: Digital watermarking, Data hiding, Classified vector quantization.

---

1. **Introduction.** With the rapid development of computer and Internet technologies, digital images can be easily created, edited and transmitted. On the one hand, the copyright of the digital image is hard to be protected since it can be perfectly replicated. On the other hand, the content of the digital image is hard to be authenticated since it can be easily tampered by software. Under these backgrounds, digital watermarking emerges. Watermarking is the procedure of hiding secret information called digital watermark in a carrier signal [1]. Digital watermarks can be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. Digital image watermarking algorithms can be roughly classified into three categories. The first category embeds watermarks in the spatial domain by directly changing pixel values [2]. The second category embeds watermarks by modifying the coefficients in transform domains [3, 4, 5]. The third category embeds watermarks in the compressed domains, such as JPEG [6], vector quantization (VQ) [7, 8, 9, 10, 11, 12, 13] and block truncation coding (BTC) [14, 15]. This Letter focuses on VQ-based image watermarking schemes, whose main idea is to carry watermark information by VQ codeword indices. The first non-blind robust scheme was proposed by Lu and Sun in 2000 [7], where the codebook partition technique

is used. The first blind robust scheme was also proposed by Lu et al. in 2000 [8], where codeword expansion is adopted. The first blind semi-fragile scheme was still proposed by Lu et al. in 2003 [9] based on the so-called index-constrained VQ. Furthermore, Lu et al. proposed an effective multipurpose image watermarking scheme based on multistage vector quantization in 2005 [10].

Most of existing VQ-based watermarking schemes do not consider the characteristics of each block, thus the embedding process is not adaptive. In this Letter, we propose a new blind VQ-based image watermarking method, where a special codebook named classified-codeword-labeled-codebook (CCLC) is utilized. In our scheme, the watermark can be effectively and adaptively embedded into the cover image with satisfactory invisibility in less time and can be extracted blindly. Experimental results demonstrate that our scheme is with not only good invisibility but also high robustness to many content preserving image processing operations.

2. **Proposed Watermarking Method.** Vector quantization (VQ) is a famous lossy compression technology that has been successfully applied in image compression and pattern recognition. VQ maps the k-dimensional Euclidean space R^k into a finite codebook $C = \{\boldsymbol{c}_i, i = 0, 1, ..., N-1\}$, where $\boldsymbol{c}_i$ is a codeword with k dimensions and N is the number of codewords. For each k-dimensional input vector $\boldsymbol{x}$, the VQ quantizer searches the codeword $\boldsymbol{c}_i$ that has the least distortion to reconstruct the input vector $\boldsymbol{x}$, i.e.

$$d(\boldsymbol{x}, \boldsymbol{c}_i) = \min_{0 \le j < N} d(\boldsymbol{x}, \boldsymbol{c}_j) \tag{1}$$

where $d(\boldsymbol{x}, \boldsymbol{c}_j)$ denotes the mean square error (MSE) between $\boldsymbol{x}$ and $\boldsymbol{c}_j$.

In our watermarking scheme, we suppose that $\boldsymbol{Y}$ is the original gray-level image of size $P \times Q$, where each pixel is with G bits, that is

$$\boldsymbol{Y} = \{y_{ij}, 0 \le i < P, 0 \le j < Q\} \tag{2}$$

where $y_{ij} \in \{0, 1, 2, ..., 2^G - 1\}$ is the gray value of the pixel located at (i, j) in $\boldsymbol{Y}$. Furthermore, we suppose that $\boldsymbol{W}$ is a visually recognizable binary watermark of size $A \times B$, that is

$$\boldsymbol{W} = \{w_{ij}, 0 \le i < A, 0 \le j < B\} \tag{3}$$

where $w_{ij} \in \{0, 1\}$ is the binary value of the watermark pixel located at (i, j) in $\boldsymbol{W}$. Our watermarking scheme contains three stages. The first stage is to generate a special codebook named CCLC. The second stage is to embed a watermark in the cover image based on the generated CCLC. The third stage is to extract the watermark from the suspect watermarked image based on CCLC. The detailed procedures can be illustrated as following three subsections.

2.1. **Classified-Codeword-Labeled Codebook Generation.** In order to implement our watermark embedding and extraction procedures, the first task is to generate a suitable codebook. In this Letter, we adopt four 256 grayscale images of size 512 × 512 as training images. Each image is divided into non-overlapping blocks of size 4 × 4, i.e., $k = 16$. To achieve both adaptive embedding and blind extraction of the robust watermark, unlike the traditional VQ codebook generation process, we generate a special codebook with classified and labeled codewords, which is called CCLC in short. That is, each codeword in the designed codebook has its exclusive class and label, respectively. In this Letter, we view the class information of all codewords as one embedding key, key_1, and the label information as the other embedding key, key_2. The codebook generation procedure can be illustrated as follows:

Step 1: Input all of the training vectors into the classifier to divide them into four groups. The first group consists of all bright detailed blocks (BD). The second group consists of all dark detailed blocks (DD). The third group consists of all bright smooth blocks (BS). The last group consists of all dark smooth blocks (DS). Here, We adopt the block-wise average gray level and deviation to denote the brightness and smoothness of each block. And in the simulation, we choose 140 and 20 as their threshold values, correspondingly.

Step 2: For each group, we perform following three substeps.

Step 2.1: Use the LBG algorithm to generate an initial codebook that is just with half-size of the one we will finally obtain.

Step 2.2: Partition the vectors in each cell into two parts by the LBG algorithm to get two new cells replacing the original one.

Step 2.3: Randomly label the centroids (i.e. the codewords) of the two cells from the same initial cell as 0 and 1, respectively. Thus, the two codewords from the same initial cell have different labels.

Step 3: Finally, we obtain four codebooks corresponding to four groups, where the numbers of codewords in four codebooks are denoted as N_0, N_1, N_2 and N_3 respectively. Here, 0 stands for BD, 1 for DD, 2 for BS and 3 for DS respectively.

2.2. **The Embedding Procedure.** With the CCLC in hand, the process of embedding the watermark $\boldsymbol{W}$ into the original image $\boldsymbol{Y}$ can be illustrated as follows.

Step 1: To eliminate the spatial correlation of neighboring watermark bits and improve the robustness against image cropping, we perform the pseudo-random permutation on $\boldsymbol{W}$.

$$\begin{aligned} \boldsymbol{W}_{\mathtt{P}} &= \mathtt{Permutaion}\{\boldsymbol{W}\} \\ &= \{w_{\mathtt{P}ij} = w_{i'j'}, 0 \le i, i' < A, 0 \le j, j' < B\} \end{aligned} \tag{4}$$

Step 2: Segment the original image Y into $\frac{1}{4}P \times \frac{1}{4}Q$ blocks of size 4×4, where $\frac{1}{4}P \ge A$ and $\frac{1}{4}Q \ge B$, so that we can embed each bit of the watermark into an exclusive block. The segmentation can be described as

$$\begin{aligned} \boldsymbol{Y} &= \{\mathbf{y}^{ij}, 0 \le i < \frac{1}{4}P, 0 \le j < \frac{1}{4}Q\} \\ &= \{y_{4i+m,4j+n}, 0 \le i < \frac{1}{4}P, 0 \le j < \frac{1}{4}Q, \\ &\quad 0 \le m < 4, 0 \le n < 4\} \end{aligned} \tag{5}$$

where $\mathbf{y}^{ij}$ can be viewed as a 16-dimensional vector.

Step3: For each input vector $\mathbf{y}^{ij}$, the embedding process can be illustrated as following substeps:

Step 3.1: Input $\mathbf{y}^{ij}$ into the classifier to judge the class which it belongs to, where the class index is denoted as t_{ij} (0 for BD, 1 for DD, 2 for BS and 3 for DS).

Step 3.2: Input $\mathbf{y}^{ij}$ together with the class index t_{ij} into the VQ encoder. From the t_{ij}-th codebook, the quantizer finds the nearest codeword of $\mathbf{y}^{ij}$ whose label is equal to the watermark bit $w_{\mathtt{P}ij}$. Thus, we can obtain the watermarked image block as follows:

$$\tilde{\mathbf{y}}^{ij} = \mathbf{c}_l^{t_{ij}} \tag{6}$$

where $\mathbf{c}_l^{t_{ij}}$ denotes the codeword in the t_{ij}-th codebook satisfying:

$$d(\mathbf{c}_l^{t_{ij}}, \boldsymbol{y}^{ij}) = \min_{0 \le n < N_{t_{ij}}} \{d(\mathbf{c}_n^{t_{ij}}, \boldsymbol{y}^{ij}), \mathtt{label}\{\mathbf{c}_n^{t_{ij}}\} = w_{\mathtt{P}ij}\} \tag{7}$$

where $N_{t_{ij}}$ is the number of codewords in the t_{ij}-th codebook and $\texttt{label}(\boldsymbol{c})$ is a function to check the label of the codeword $\boldsymbol{c}$.

Step 4: Obtain the watermarked image $\tilde{\boldsymbol{Y}}$ by assembling all of the watermarked image blocks.

2.3. **The Extraction Procedure.** The watermark extraction of our scheme is very simple and fast. In addition, it can be performed blindly, that is, we do not require the original image. From a suspect image $\boldsymbol{Y}^*$ of size $P \times Q$, we can extract the watermark $\boldsymbol{W}^*$ based on following steps:

Step 1: Segment the suspect image $\boldsymbol{Y}^*$ into blocks of size 4×4, i.e.,

$$\begin{aligned}\boldsymbol{Y}^* &= \{\mathbf{y}^{*ij}, 0 \le i < \frac{1}{4}P, 0 \le j < \frac{1}{4}Q\} \\ &= \{y^*_{4i+m,4j+n}, 0 \le i < \frac{1}{4}P, 0 \le j < \frac{1}{4}Q, \\ &\quad 0 \le m < 4, 0 \le n < 4\} \end{aligned} \tag{8}$$

Step 2: For each input vector $\mathbf{y}^{*ij}$, the extraction process can be illustrated as following substeps:

Step 2.1: Input $\mathbf{y}^{*ij}$ into the classifier to judge the class which it belongs to, where the class index is denoted as t^*_{ij} .

Step 2.2: Input $\mathbf{y}^{*ij}$ together with the class index t^*_{ij} into the VQ encoder. From the t^*_{ij}-th codebook, the quantizer finds the nearest codeword of $\mathbf{y}^{*ij}$ satisfying:

$$d(\mathbf{c}_l^{t^*_{ij}}, \boldsymbol{y}^{*ij}) = \min_{0 \le n < N_{t^*_{ij}}} \{d(\mathbf{c}_n^{t^*_{ij}}, \boldsymbol{y}^{*ij})\} \tag{9}$$

where $N_{t^*_{ij}}$ is the number of codewords in the t^*_{ij}-th codebook.

Step 2.3: Check the label of as the extracted watermark bit, i.e.,

$$w^*_{\mathtt{P}ij} = \texttt{label}\{\mathbf{c}_l^{t^*_{ij}}\} \tag{10}$$

Step 3: Assemble all the extracted watermark bits $w^*_{\mathtt{P}ij}$ to obtain a watermark $\boldsymbol{W}^*_{\mathtt{P}}$ and then perform the inverse pseudo-random permutation on $\boldsymbol{W}^*_{\mathtt{P}}$ to obtain the final extracted watermark $\boldsymbol{W}^*$.

3. **Experimental Results.** To evaluate the performance of the proposed watermarking technique, the 512×512 Lena image with 8bit/pixel resolution is used as the cover image for watermarking test. In the experiments, we adopt four 256 grayscale images of size 512×512 including Lena, Peppers, F16 and Girl, as training images to generate four codebooks, whose numbers of codewords are 452, 114, 358, 100 corresponding to Class BD, Class DD, Class BS, and Class DS respectively. Here, we can easily see that the total number of codewords is 1024. The watermark $\boldsymbol{W}$ is a binary image of size 128×128. Fig.1 shows the original Lena image and Fig.2 shows the watermarked Lena image with PSNR=31.45dB. And the processing time of the embedding algorithm is generally about 5 seconds.To verify the robustness of the proposed algorithm, we perform several attacks on the watermarked image $\tilde{\boldsymbol{Y}}$, including VQ compression with the same codebook used by the embedding process, JPEG compression with QF =90, JPEG compression with QF =80, image cropping in the upper-left quarter, median filtering with a 3×3 window, blurring, sharpening, adding Gaussian noise by 1%, and rotation by 0.1°.The corresponding extracted watermark $\mathbf{W}^*$ is shown in Fig.3(a)-(k), the original watermark is shown in Fig.3(a) and the extracted watermark under no attacks is shown in Fig.3(b). The performance of the extracted watermark is evaluated by Normalized Cross-correlation (NC).

Figure 1. Original Lena image

Figure 2. Watermarked image with PSNR=31.45dB

From these results, we can see that the proposed algorithm is considerably helpful in meeting the expectation of robustness watermarking. In addition, the proposed algorithm is blind because we do not require the original image in watermark extraction. Furthermore, the security of our scheme is guaranteed by two embedding keys key_1 and key_2 together with the watermark permutation key.

To further show the superior of the proposed scheme over the existing scheme in [12], we compare them based on the Lena image and the same codebook size 1024. Experimental results show that the PSNR of the watermarked image by the scheme in [12] is 30.68dB, which is worse than the proposed scheme. In addition, the scheme in [12] takes more time to generate the watermarked image than the proposed scheme. Table 1 shows the comparison results of the robustness under the same attacks as given in Fig.3. We can see that our scheme is more robust than the method in [12].

4. **Conclusions.** A novel robust digital watermarking scheme based on Classified-Labeled-Codeword VQ is proposed. It is blind and effective. According to the experimental results under various kinds of attacks, we are able to assert its robustness, which is superior to some existing algorithms. And because it adopts vector-classifying, the embedding process is less time-consuming and more efficient than the normal VQ-based method. In a

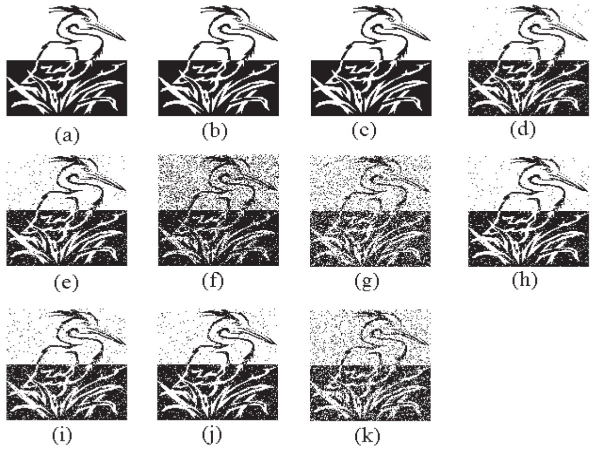

Figure 3. Original watermark and extracted watermarks. (a)Original watermark $\boldsymbol{W}$;(b)No attack, NC =1.0000;(c)VQ, NC =1.0000;(d)JPEG, QF=90, NC =0.9814;(e)JPEG, QF=80, NC =0.9725;(f)Image cropping, NC =0.7378;(g)Median filtering NC=0.7306;(h)Blurring, NC=0.9557;(i)Sharpening, NC=0.9064; (j)Gaussian noise 1%, NC=0.9602;(k)Rotation by 0.1°, NC =0.7870.

Table 1. Comparisons of robustness (NC) between the proposed scheme and the VQ-based watermarking method[12]

attacks	**the proposed scheme**	**the scheme in [12]**
No attack	1.0000	1.0000
VQ re-encoding	1.0000	1.0000
JPEG with QF=80	0.9725	0.8351
Image cropping	0.7378	0.7170
Median filtering	0.7306	0.6651
Blurring	0.9557	0.6502
Sharpening	0.9064	0.9048
1% Gaussian noise	0.9602	0.9010
Rotation by 0.1°	0.7870	0.7530

word, our scheme is a robust, blind and fast watermarking scheme which can be applied to the application of copyright protection.

Acknowledgments. This work is supported by the National Natural Science Foundation of China under grant 61171150, and also supported by Zhejiang Provincial Natural Science Foundation of China under grant R1110006 and Special Fund on Strategic New Industry Development of Shenzhen under grant JCYJ20120817163934173.

References

[1] I. J. Cox, Digital watermarking and steganography, *Morgan Kaufmann*, Burlington, MA, USA, 2008.
[2] D. P. Mukherjee, S. Maitra, and S. T. Acton, Spatial domain digital watermarking of multimedia objects for buyer authentication, *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 1–15, 2004.
[3] G. Feng, and Y. M. Yang, Adaptive DCT based digital watermarking scheme, *Applied Mechanics and Materials*, vol. 20-23, no. 1, pp. 1136–1142, 2010.

[4] S. Emek, M. Pazarci, and M. Yucel, A DWT-DCT based digital Watermarking Technique, *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference*, pp. 33-36, Apr. 2004.

[5] H. Luo, F. X. Yu, Z. L. Huang, and Z. M. Lu, Blind image watermarking based on discrete fractional random transform and subsampling, *Optik - International Journal for Light and Electron Optics*, vol. 122, no. 4, pp. 311–316, 2011.

[6] V. Saxena, and J. P. Gupta, A novel watermarking scheme for JPEG images, *WSEAS Transactions on Signal Processing*, vol. 2, no. 2, pp. 74–84, 2009.

[7] Z. M. Lu, and S. H. Sun, Digital image watermarking technique based on vector quantisation, *Electronics Letters*, vol. 36, no. 4, pp. 303–305, 2000.

[8] Z. M. Lu, J. S. Pan, and S. H. Sun, VQ-based digital image watermarking method, *Electronics Letters*, vol. 36, no. 14, pp. 1201-1202, 2000.

[9] Z. M. Lu, C. H. Liu, D. G. Xu, and S. H. Sun, Semi-fragile image watermarking method based on index constrained vector quantisation, *Electronics Letters*, vol. 39, no. 1, pp. 35-36, 2003.

[10] Z. M. Lu, D. G. Xu, and S. H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, *IEEE Transactions on Image Processing*, vol. 14, no. 6, pp. 822–831, 2005.

[11] H. C. Huang, F. H. Wang, and J. S. Pan, A VQ-based Robust Multi-watermarking Algorithm, *IEICE Transactions on Fundamental*, vol. E85-A, no. 7, pp. 1719–1726, 2002.

[12] Z. M. Lu, W. Xing, D. G. Xu, and S. H. Sun, Digital image watermarking method based on vector quantization with labeled codewords, *IEICE Transactions on Information and Systems*, vol. E86-D, no. 12, pp. 2786–2789, 2003.

[13] H. X. Wang, Z. M. Lu, Y. N. Li, and S. H. Sun, A Compressed domain multipurpose video watermarking algorithm using vector quantization, *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 10, pp. 1441–1450, 2009.

[14] Z. M. Lu, C. H. Liu, and S. H. Sun, Digital image watermarking technique based on block truncation coding with vector quantization,*Chinese Journal of Electronics*, vol. 11, no. 1, pp. 152–157, 2002.

[15] C. N. Yang, and Z. M. Lu, A blind image watermarking scheme utilizing BTC bitplanes, *International Journal of Digital Crime and Forensics*, vol. 3, no. 6, pp. 42–53, 2011.