INFORMATICA, 2004, Vol. 15, No. 2, 147–160

VQ-Based Image Watermarking Using Anti-Gray Coding

Chin-Chen CHANG, Hsien-Wen TSENG
Department of Computer Science and Information Engineering
National Chung Cheng University
Chaiyi, Taiwan 621, R.O.C.
e-mail: {ccc,hwtseng}@cs.ccu.edu.tw

Received: August 2003

Abstract. In this paper, a new digital watermarking method based on vector quantization (VQ) is proposed. In contrast with conventional VQ-based watermarking schemes, the mean of sub-blocks is used to train the VQ codebook. In addition, the Anti-Gray Coding (AGC) technique is employed to enhance the robustness of the proposed watermarking scheme. In this scheme, the secret keys are used to hide the associated information between the original image and the watermark. Then the set of secret keys will be registered to a trusted third party for future verification. Thus, the original image remains unchanged after the watermark is melted into the set of secret keys. Experimental results show that the watermark can survive various possible attacks. Besides that, the size of the secret keys can be reduced.

Key words: vector quantization, digital watermarking, pseudo-gray coding, anti-gray coding.

1. Introduction

Due to the astonishingly rapid growth of the Internet, the hard-to-restrain copying and easy distribution of digital images online have made copyright protection a tough task to accomplish. To deal with this problem, over the past years, a lot of research resources have been devoted to the development of new digital watermarking techniques. Generally speaking, digital watermarking is a technique with which one or more watermarks can be embedded into the digital contents and/or into the secret keys for copyright protection. The embedded watermarks can be extracted later from the watermarked contents and/or the secret keys for future verification.

Most of the earlier watermarking techniques were based on the spatial domain, the simplest form functioning by modifying the least significant bit (LSB) of the pixel value (Van Schyndel *et al*., 1994). Then some other techniques were developed that transform from the spatial domain to the frequency domain (Cox *et al*., 1997; Hsu and Wu, 1999). In addition, Vector-Quantization-based (VQ-based) watermarking schemes were also released in research papers such as (Lu and Sun, 2000; Huang *et al*., 2002). Relatively speaking, VQ-based watermarking could have only partial effect. As a result, Chang and Tsai (2000) proposed a watermarking scheme that coalesces both the VQ technique and

the technique of principle component analysis (PCA). In their scheme, the VQ codebook is sorted by PCA, so that the similar codewords get gathered together to help with the melting and extracting of the watermark. The secret keys associated with the watermark is outputted after melting and then registered to the trusted third party for future verification. In this paper, a novel VQ-based watermarking scheme is presented. In this new scheme, the Anti-Gray Coding (AGC) technique (Kuo *et al*., 1999) is employed for codebook generation so as to enhance the robustness of watermarking. The proposed technique can satisfy such requirements as watermark invisibility, security, robustness, and blindness. Experimental results show that the proposed technique can survive various kinds of attacks. Besides that, the size of the secret keys is much smaller than that of Chang and Tsai's method.

This paper is organized as follows. In Section 2, both the Chang–Tsai's method and the concept of Anti-Gray Coding are reviewed. Then, the proposed algorithm would be presented in Section 3, followed by the experimental results in Section 4. Finally, the conclusions would be in Section 5.

2. Related Works

2.1. *Chang and Tsai's Method*

In Chang and Tsai's scheme, the first step is to generate the VQ codebook by using the LBG algorithm (Linde *et al*., 1980). Then the PCA technique, a quite popular dimensionality reduction technique in the field of pattern recognition, is employed to sort the codebook. Along the direction of the maximum variance, PCA projects the dimensional data into a linear subspace with a minimum loss of information. In other words, all the projection points obtained from the subspace still preserve the properties of the original information. After the codebook is sorted, the similar codewords in the sorted codebook get gathered.

In the melting process, each watermark bit will randomly match with one block in the original image. The nearest codeword in the sorted codebook is found for the block, and the index of the codeword is returned. If the watermark bit is 1, then the index will be stored in the secret key table. On the contrary, the index of a dissimilar codeword, i.e., a quite far-away index in the sorted codebook, will be stored in the secret key table when the watermark bit is 0. The secret key table is generated after all the watermark bits are processed.

Then, in the extracting process, a threshold T is set up to determine whether the watermark value is to be set as 1 or 0 in the melted block. If the index for the melted block is close to the corresponding index in the secret key table, the recovered watermark value should be 1; otherwise, the recovered watermark value should be 0.

According to their experimental results, Chang and Tsai's method is truly robust against various attacks. Besides, the method can effectively generate the secret keys without modifying the original image.

2.2. *Anti-Gray Coding*

Before reviewing AGC, Pseudo-Gray Coding (PGC) should be mentioned first. PGC is an important work proposed by Zeger and Gersho in 1990 (Zeger and Gersho, 1990). It is an index assignment scheme that can effectively reduce the average distortion by rearranging the codewords in a given VQ codebook. The codewords of the neighboring set (Hamming distance equals one) are assigned closely, such that the distances of the corrupted codewords caused by channel error are close, on average, to the original codewords. By using PGC, the VQ-encoded image can be transmitted through a noisy channel while preserving good image quality.

In AGC, the concept of PGC is completely reversed. The codewords of the neighboring set are assigned as far as possible, such that the distances of corrupted codewords caused by channel error differing greatly from the original codewords. As a result, the noisy blocks become obvious and can be easily detected and corrected.

Now the concept of AGC is used to enhance the robustness of the proposed watermarking scheme. Assume that the VQ codebook is reassigned using AGC and that the distances between neighbors are far apart. In an attacked image, the pixels are probably modified. Since the distances among the neighboring set are far apart, the attacked block stands a good chance of recovering its original self except for large distortion.

3. The Proposed Algorithm

Let X be the original gray-level image of size $M_1 \times M_2$, and the digital watermark W be a binary image of size $W_1 \times W_2$. First, the watermark W is to be melted into the original image X, and then the secret keys associated with the watermark are to be outputted. The secret keys are then registered to the trusted third party for certifying the ownership of the original image. In this section, the melting procedure is presented and the extracting procedure will be proposed accordingly.

3.1. *The Melting Procedure*

To melt the binary watermark into a set of secret keys, it must have a codebook first. Several image sources are given for training the codebook. The images are decomposed into blocks of 4×4, and then each block is divided into 4 sub-blocks as shown in Fig. 1.

The mean of each sub-block is calculated, and a vector with 4 dimensions is produced. This results in a training set consisting of large source vectors. Then the LBG algorithm (Linde *et al.*, 1980) is employed to generate a codebook C with size N, where $C = \{c_0, c_1, \ldots, c_{N-1}\}$ and $N = 2^n$, $n > 0$. After the codebook C is generated, AGC is applied for index reassignment. The codewords among the neighboring set (Hamming distance equals one) are assigned as far as possible, such that the distances among these codewords differ greatly. The aim for this is to enhance the robustness of watermark. It will be discussed later.

10	12	12	14
10	8	8	14
20	24	20	20
24	20	20	20

(a) Four sub-blocks decomposed from a 4×4 block

10	12
22	20

(b) Four means obtained from four sub-blocks

Fig. 1. Example of block decomposition.

Then the binary watermark will be melted into the original image to produce the secret keys. As is usually the case, the original image X is first divided into blocks of 4×4, and the means of the 4 sub-blocks are separately computed. Assume that the digital watermark W is expressed as a bit stream with every $\log_2 n$ bits translated into an integer, say $W = \{w_0, w_1, \ldots, w_{T-1}\}$, where $T = (W_1 \times W_2)/\log_2 n$ and $0 \leqslant w_i \leqslant n-1$. Then the secret key generation process can be described as follows:

1. Pick out T blocks from the original image X by using a pseudo-random number generator with a seed S.
2. For each block x_i in T, find the nearest codeword c_{α_i} from codebook C, and use the index α_i to represent the block.
3. Melt the watermark value w_i into the block x_i to generate key_i by complementing the w_i-th bit of x_i's corresponded index α_i. The bit order is from LSB to MSB, numbered 0 to $n-1$. For example, if $n = 4,\ \alpha_i = 8 = 1000_2$, and $w_i = 2$, then the secret key $key_i = 1100_2 = 12$.
4. Finally, the set K of secret keys key_i's for the original image X is produced. $K = \{key_0, key_1, \ldots, key_{T-1}\}$.

After the secret keys are produced, the watermark W and the set K of secret keys are then registered to the trusted third party for protecting the ownership of the original image. Since the watermark is not directly embedded into the original image, the watermarked image stays free from distortions.

The block diagram for melting watermarks is depicted in Fig. 2.

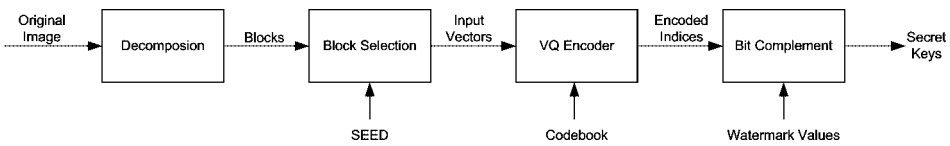

Fig. 2. The block diagram for watermarking.

3.2. *The Extracting Procedure*

The extraction of the watermark requires the set K of secret keys, the seed S, and the digital image X'. The extraction steps are as follows:

1. Find the ordered set of blocks, T, from the image X' using the seed S.
2. For each block y_i in T, find the nearest codeword c_{β_i} from the codebook C, and use the index β_i to represent the block.
3. Perform the exclusive-or (XOR) operation on index β_i and key_i to obtain the Hamming distance d between index β_i and key_i.

Index β_i and key_i are expected to have a Hamming distance of one. If so, assume the position of the different bit is located in bit w_i', and then the watermark can be obtained by translating w_i' to a binary string sized $\log_2 n$. For example, if $n = 4,\ \beta_i = 8 = 1000_2$, and $key_i = 12 = 1100_2$, then index β_i and key_i have a Hamming distance of one, and the different bit is located in bit 2. Translating the value 2 to a binary string sized $\log_2 n = 2$, and the extracted watermark value "10" is obtained.

In case a Hamming distance d greater than one, the block y_i is probably quite distorted. To recover the watermark, the neighboring set of key_i (the set of indices that have Hamming distances equal to one from key_i) in the codebook C is computed. Then, the nearest codeword c_{β_i} is found in the neighboring set for the block y_i and use index β_i to represent the block. This way, the watermark value can be extracted as in the case of Hamming distance d equaling one.

Since the codebook C is rearranged by using Anti-Gray Coding (AGC), the average distortion is large enough among the neighboring set. As long as a block y_i is not degraded completely, the extracting procedure has a good chance to recover the watermark value successfully. For example, if $key_i = 12 = 1100_2$, then the neighboring set of key_i is $\{0100_2, 1000_2, 1110_2, 1101_2\}$. Since the corresponding codewords in the set are assigned as far as possible, the block y_i has a good chance of recovering its original block 1000_2 unless the block y_i is severely degraded.

The block diagram for the extraction procedure is shown in Fig. 3.

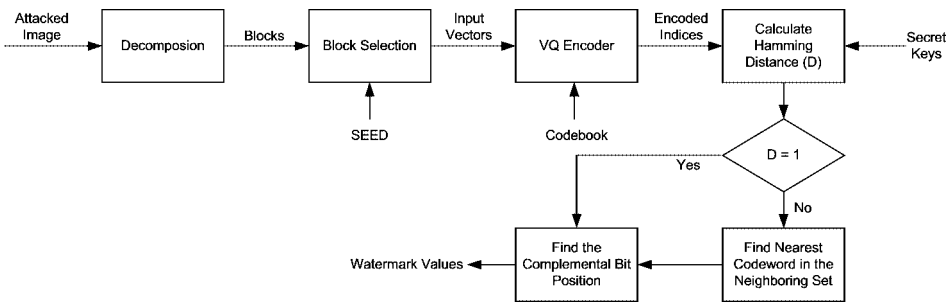

Fig. 3. The block diagram for extracting watermark.

3.3. *Comparison with Related Work*

Both Chang and Tsai's scheme and the proposed algorithm are VQ-based image watermarking methods. Before melting the watermark into an original image, these two methods construct a VQ codebook and sort the codebook using different techniques. Chang and Tsai use the PCA technique to sort the codebook such that the similar codewords are put gather. However, in the proposed approach, the AGC algorithm is applied to the codebook for index reassignment such that the codewords in the neighboring set are assigned as far as possible. The reason for sorting the codebook is to enhance the robustness of watermarking. For a codebook with size N and a block with size 4×4, Chang and Tsai's codebook uses 16-dimension code vector, while ours uses only 4-dimension code vector. Thus the memory space required by the codebook in the proposed method is only one fourth of that in Chang and Tsai's method. Besides, in the melting procedure, the number of watermark bits melted into the secret key is different in these two methods. Chang and Tsai's method uses one index to represent one watermark bit. In the proposed method, $\log_2 n$ watermark bits can be melted into an index, where n is the length of each index. For example, if the codebook contains 256 codewords, then the size of each index is 8 and three watermark bits can be melted into an index. Thus the size of secret keys in the proposed method is only one third of that in Chang and Tsai's method. In brief, the two schemes use different techniques to enhance the robustness of watermarking. It is obvious that the extra memory space required by the proposed method is less than that required by Chang and Tsai's.

4. Experimental Results

Five gray-level images Lena, Barbara, Baboon, F16, and Pepper with size 512×512 are used as the test images in the experiments. The watermark image is a binary image with 64×64 pixels as shown in Fig. 4. The effectiveness of the extracted watermark is evaluated by Bit Correction Rate (BCR). The similarity measurement between the original watermark W and the extracted one W' is defined as

$$BCR = \frac{\sum_{i=0}^{W1-1}\sum_{j=0}^{W2-1}\left[\overline{W(i,j)\oplus W'(i,j)}\right]}{W_1 \times W_2} \times 100\%.$$

To verify the robustness of the proposed method, several attacks are applied on the original image Lena. The attacks include JPEG lossy compression, blurring, sharpening, cropping, and rotating. In the first experiment, the codebook C sized 256 is obtained by the LBG algorithm and is rearranged using AGC, which corresponds to 8 bits per index. Thus three watermark bits can be melted into each selected block and the secret key size is $\frac{64\times64}{3} \times 8$ bits. Table 1 summarizes the results after attacks using the proposed method and Table 2 shows the results after attacks using Chang and Tsai's method. It can be observed that the proposed method can do just as well as Chang and Tsai's method. However, the secret key size of the proposed method is only one-third of that in Chang

Table 1
Results after attacks using the proposed method (codebook size 256)

Attacks	Lena	Barbara	Baboon	F16	Pepper
JPEG (14:1)	99.48%	98.36%	97.01%	96.21%	99.24%
JPEG (25:1)	93.92%	94.97%	91.67%	91.26%	96.78%
JPEG (35:1)	87.81%	87.62%	87.96%	87.11%	95.09%
Blurring	99.44%	99.23%	95.82%	98.36%	98.73%
Sharpening	99.02%	97.92%	99.19%	97.92%	98.14%
Cropping	86.67%	92.38%	89.21%	87.52%	87.64%
Rotating (1°)	92.72%	92.10%	88.74%	83.80%	95.16%
Rotating (2°)	87.81%	88.04%	86.10%	81.63%	92.03%

Table 2
Results after attacks using Chang and Tsai's method (codebook size 256)

Attacks	Lena	Barbara	Baboon	F16	Pepper
JPEG (14:1)	99.95%	98.38%	97.23%	96.28%	99.25%
JPEG (25:1)	93.50%	94.98%	92.00%	91.54%	96.64%
JPEG (35:1)	87.65%	87.71%	87.86%	87.62%	94.68%
Blurring	99.95%	99.35%	95.71%	98.33%	98.56%
Sharpening	99.78%	98.06%	99.08%	97.88%	98.28%
Cropping	86.40%	92.58%	89.25%	88.14%	88.02%
Rotating (1°)	93.65%	92.87%	89.19%	84.26%	95.74%
Rotating (2°)	88.12%	88.19%	87.07%	82.19%	92.95%

and Tsai's method. The reason is that the proposed method hides three bits per index, whereas Chang and Tsai's method hides only one bit per index.

In the second experiment, the proposed method uses a codebook C sized 16, thus the index size is 4 bits. Then two watermark bits can be melted into each selected block and the secret key size is $\frac{64\times64}{2} \times 4$ bits. Table 3 shows the BCR values of the extracted watermark after several attacks. It can be seen that the results are better than that of codebook sized 256.

Table 3
Results after attacks using the proposed method (codebook size 16)

Attacks	Lena	Barbara	Baboon	F16	Pepper
JPEG (14:1)	99.85%	99.32%	98.65%	99.41%	99.83%
JPEG (25:1)	99.48%	99.15%	97.95%	99.01%	99.68%
JPEG (35:1)	98.34%	98.02%	97.31%	98.22%	99.22%
Blurring	99.85%	99.68%	98.80%	99.80%	99.80%
Sharpening	99.58%	99.49%	99.17%	99.24%	99.80%
Cropping	97.19%	96.67%	97.44%	97.63%	98.88%
Rotating (1°)	95.07%	94.56%	93.02%	94.75%	94.80%
Rotating (2°)	93.83%	92.44%	92.58%	94.14%	94.11%

(a) Original image Lena.

(b) The original watermark.

(c) The extracted watermark.

Fig. 4. The original image, the original watermark, and the extracted watermark.

4.1. *No Attack*

Fig. 4 shows the original image Lena, the original watermark, and the extracted watermark when no attack is applied. It can be seen that $BCR = 100\%$, and this means the extracted watermark and the original watermark are identical.

4.2. *JPEG Compression Attack*

Fig. 5 shows the JPEG-attacked images and the extracted results after JPEG lossy compression with the compression rate being 14:1, 25:1 and 35:1. From the experimental result, it can be seen that the extracted watermark is still highly similar to the original watermark.

4.3. *Spatial-Domain Attacks*

Four spatial-domain attacks are used to verify the robustness of the proposed watermark algorithm. The four attacks include blurring, sharpening, cropping, and rotating. Fig. 6 shows a blurred version of the image and the extracted watermark. A simple two-dimensional low-pass filter operation is used for blurring. The filter can be defined in the form:

$$\begin{bmatrix} 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \end{bmatrix}.$$

The original image is applied by taking the value of a pixel and all eight of its immediate neighbors, dividing them each by nine and adding them together to obtain the new value for the pixel. As regards the sharpening attack, a simple two-dimensional high-pass

(a) JPEG-attacked image (14:1).

(b) The extracted watermark.

(c) JPEG-attacked image (25:1).

(d) The extracted watermark.

(e) JPEG-attacked image (35:1).

(f) The extracted watermark.

Fig. 5. JPEG attack.

(a) Blurring-attacked image.

(b) The extracted watermark.

Fig. 6. Blurring attack.

(a) Sharpening-attacked image.

(b) The extracted watermark.

Fig. 7. Sharpening attack.

filter operation is used. The operation is performed by constructing a copy of the original image, applying a blurring operation to it, and then subtracting the pixel values in this blurred image from the corresponding values in the original multiplied by a scaling factor of 2. The results of the sharpening attack are shown in Fig. 7. Besides, Fig. 8 shows a cropped image and the extracted watermark. Since pseudo-random selection is applied, the lost information will be distributed over the whole image, and the error will also be distributed over the whole result. Fig. 9 shows the image that rotates one degree and two degree in clockwise direction and the extracted watermarks. From the experimental results, it can be seen that the extracted watermark can still be clearly recovered after various attacks.

(a) Cropping-attacked image.

(b) The extracted watermark.

Fig. 8. Cropping attack.

(a) Rotating-attacked image (1°).

(b) The extracted watermark.

(c) Rotating-attacked image (2°).

(d) The extracted watermark.

Fig. 9. Rotating attack.

5. Conclusions

In this paper, a new watermarking scheme that satisfies such requirements as invisibility, security, robustness, and blindness is proposed. The proposed scheme can effectively melt the watermark without modifying the original image. Basically, this approach is to hide the associated information between the original image and the watermark into the secret keys. Then the secret keys will be registered to the trusted third party for future verification. It can be obviously seen that after the watermark is melted into the set of secret keys, the original image remains unchanged.

In addition, AGC is applied to the VQ codebook for index reassignment, such that the codewords in the neighboring set are assigned as far as possible. In this way, the robustness of watermarking can be improved. The experimental results show that the proposed watermarking scheme can stand up to various kinds of attacks, demonstrating its robustness. Furthermore, the size of the secret keys can be drastically reduced comparing to that of Chang and Tsai's. The proposed scheme can save two-third on the secret key size when using the VQ codebook sized 256.

References

Chang, C.-C., and C.-S. Tsai (2000). A technique for computing watermarks from digital images. *Informatica*, **24**(3), 391–396.

Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Processing*, **6**(12), 1673–1687.

Hsu, C.-T., and J.-L. Wu (1999). Hidden digital watermarks in images. *IEEE Trans. Image Processing*, **8**(2), 58–68.

Huang, H.-C., F.-H. Wang and J.-S. Pan (2002). A VQ-based robust multi-watermarking algorithm. *IEICE Trans. Fundamentals*, **E85-A**(7), 1719–1726.

Kuo, C.-J., C.-H. Lin and C.-H. Yeh (1999). Noise reduction of VQ encoded images through Anti-Gray coding. *IEEE Trans. Image Processing*, **8**(1), 33–40.

Linde, Y., A. Buzo and R.M. Gray (1980). An algorithm for vector quantizer design. *IEEE Trans. Communications*, **COM-28**, 84–95.

Lu, Z.-M., and S.-H. Sun (2000). Digital image watermarking technique based on vector quantisation. *Electronics Letters*, **36**(4), 303–305.

Van Schyndel, R.G., A.Z. Tirkel, N. Mee and C.F. Osborne (1994). A digital watermark. In *Proceedings of IEEE International Conference on Image Processing*, Austin, Texas, USA, Vol. 2. pp. 86–90.

Zeger, K., and A. Gersho (1990). Pseudo-Gray coding. *IEEE Trans. Communications*, **38**, 2147–2158.

C.-C. Chang was born in Taichung, Taiwan, on Nov. 12, 1954. He received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision science in 1979 from National Tsing Hua University, Hsinchu, Taiwan. He received his PhD degree in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to 1989, he was among the faculty of Institue of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he was worked as a professor of Institute of Computer Science and Information Engineering at National Chung Cheng University, Chaiyi, Taiwan. Dr. Chang is a fellow of IEEE and a member of Chinese Language Computer Society, Chinese Institute of Engineers of Republic of China, and Phi Tau Phi Society of Republic of China. His reaserch interests include computer cryptography, data engineering, and image compression.

H.-W. Tseng received the BS degree in computer science and information engineering from Tamkang University, Taipei County, Taiwan, in 1986, and his MS degree in computer science and information engineering from National Taiwan University, Taipei, Taiwan, in 1988. Since 1989 to 2000, he was worked as an computer engineer. He is currently working toward to the PhD degree in computer science and information engineering at National Chung Cheng University, Chaiyi, Taiwan. His research interests include image processing, data hiding, and error resilient coding.

Vektorių kvantavimu grindžiamas vaizdų fono raštų kūrimas, naudojant pilkumui atsparų kodavimą

Chin-Chen CHANG, Hsien-Wen TSENG

Straipsnyje siūlomas naujas skaitmeninis vaizdų fono raštų kūrimo metodas, naudojantis slaptus raktus ryšiams tarp pradinio vaizdo ir fono rašto slėpti. Eksperimentų rezultatai rodo, kad tokie fono raštai atsparūs ivairioms galimoms dekodavimo atakoms, o taip pat, kad raktų dydis gali būti sumažintas.