# Data Hiding by Vector Quantization in Color Image

Yung-Gi Wu

Abstract—With the growing of computer and network, digital data can be spread to anywhere in the world quickly. In addition, digital data can also be copied or tampered easily so that the security issue becomes an important topic in the protection of digital data. Digital watermark is a method to protect the ownership of digital data. Embedding the watermark will influence the quality certainly. In this paper, Vector Quantization (VQ) is used to embed the watermark into the image to fulfill the goal of data hiding. This kind of watermarking is invisible which means that the users will not conscious the existing of embedded watermark even though the embedded image has tiny difference compared to the original image. Meanwhile, VQ needs a lot of computation burden so that we adopt a fast VQ encoding scheme by partial distortion searching (PDS) and mean approximation scheme to speed up the data hiding process.

The watermarks we hide to the image could be gray, bi-level and color images. Texts are also can be regarded as watermark to embed. In order to test the robustness of the system, we adopt Photoshop to fulfill sharpen, cropping and altering to check if the extracted watermark is still recognizable. Experimental results demonstrate that the proposed system can resist the above three kinds of tampering in general cases.

**Keywords**—Data hiding, vector quantization, watermark.

#### I. INTRODUCTION

OVER the past 4000 years, there are many security techniques used for national defense and military purposes. In the recent years, due to the promising developments in business, the computer and network become one of the most frequent used media for communication. Data communication by way of network is convenient for the user; however, the data transmitted in the network is easy to be stolen or recognized if without packaging or processing furthermore.

Digital watermarking is the process of embedding information into a digital signal. The signal may be any form of the following alternatives; text, audio, pictures or video. If the signal is copied, then the information is also carried in the copy. Therefore, hiding information into the original signal is the way to achieve the goal of privacy protection. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which declares the owner of the media. When a television broadcaster shows its logo to the corner of transmitted video, this is also a visible watermark. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it is possible to detect the hidden information). An important application of invisible watermarking is the copyright protection systems, which are intended to prevent or detect unauthorized copying of digital

Y. G. Wu is with the Department of Computer Science & Information Engineering, Chang Jung Christian University, Tainan City, 71101 Taiwan (e-mail: wyg@mail.cjcu.edu.tw).

media. Steganography is sometimes applied in digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking.

The basic idea of vector quantization is quite simple, representing sequences of input vectors with a much smaller set of pre-defined vectors, which are called codevectors (codewords). There are several ways to choose the representative codevector. Most of the methods will evaluate the distortion between input vector and all codevectors in the codebook; then the codevector with minimum distortion is selected. Indexes instead of the codevectors are sent to the receiver or to be stored in storage device. The decoder uses a table-lookup method to retrieve the codevector from codebook to reconstruct the decoded image. Its simplicity of the decoder is the primary advantage of VQ.

Formally, a vector quantization of k dimension and codebook size N can be regarded as a mapping Q from a k-dimensional space  $R^k$  to a finite subset Y of  $R^k$ . That is,  $Q:R^k \to Y$  where  $Y = \{y_i \mid i=1,2,...,N\}$  containing N codevectors is called the codebook,  $y_i$  represents the i-th codevector in Y and each  $y_i$  is k-dimension as well. If the distortion measurement used to select the best match codeword for every input k-dimensional vector  $x = (x_1, x_2, x_3,...,x_k)$  in codebook is the squared Euclidean distance, the distortion between x and  $y_i$  codeword is

$$d(x, y_i) = \sum_{j=1}^{k} (x_j - y_{i_j})^2$$
 (1)

The best match codeword  $y_{bm}$  with the minimum distance is yielded

$$d(x, y_{bm}) = \min d(x, y_i) \qquad i \in 1, 2, ..., N$$
 (2)

Transmitting the index of  $y_{bm}$  instead of the whole input vector x itself achieves the goal of compression. On the decoder side, the index of bm is used to reconstruct the original image in simple way by codewords pasting from codebook according to bm. The bit rate for the conventional VQ is

$$\frac{\log_2 N}{k}$$
 bits per pixel (bpp) (3)

The conventional VQ is given in Fig. 1.

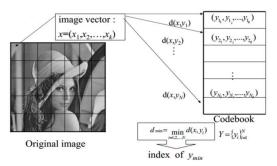


Fig. 1 Conventional VQ

The above procedure searches exhaustively through the codebook to find the best match codevector for every input vector x according to a distortion measurement as (1) and produces the associated codevector index bm. The VQ encoder with this type searching manner is called a full-search VQ (FS-VQ) [1], [2]. The computational complexity to implement FS-VQ is expensive so as to limit the application of VQ to real-time compression system. In this paper, we adopt the fast VQ encoder to increase the practical usage of this data hiding system to avoid too much processing time. In general, VQ is for compressing image to compressed form. In this paper, we use VQ to hide and retrieve data.

Due to the fast growing of information technology, the security and ownership protection of multimedia are getting more and more attention. Watermark was devised to achieve this goal. In the early age, the artists protect their own intellectual property rights of their works by signing their names within the product to indicate the authenticity of the work. If somebody who wants to remove the signature will destroy the works. Nowadays, the electronic images are easy to copy and easy to modify the features as well and human eyes are difficult to perceive the modification. Malicious attackers are capable to change the ownership or the content of the works.

The most common anti-counterfeiting watermark is on the bill that can be found by light. Some companies or manufacturers put the visible watermark covering up the picture on the bill to achieve the goal of anti-counterfeiting. However; big watermark affects content of picture and tiny watermark cannot resist the attack. The best way to protect the owner's right is embedding the digital watermark into the digital data in visible or invisible manners. The watermark to be embedded could be the company or authors' brand. If somebody wants to copy or modify the content, real owner can extract the watermark to declare his real ownership to protect the intelligent property. Reference [3] proposed a method, which is regarded as the first data hiding method for VQ-compressed images; in this scheme, two neighboring codewords are considered as a pair for embedding bits (0 and 1). In 2005, [4] proposed a reversible watermarking scheme based on modified fast correlation VQ (MFCVQ) for VQ-compressed images. However, the scheme has a considerably low hiding capacity because its embedding rate is less than 1 bit/(image block) on average. Lin et al. [5] presented an adaptive embedding technique for VQ-compressed images. They adjusted the predetermined distance threshold according to the required hiding capacity and arranged numerous similar codewords in one group to embed a secret message. Thus, on average, two bits could be embedded in each block with acceptable distortion. Wang et al. [6] presented a reversible data hiding scheme involving a combination of locally adaptive coding (LAC) and side-match VQ. In this scheme, a self-organizing sequence and an adaptive threshold list are first defined to concentrate the distribution of index positions so that the variance among the indices can be reduced. Thereafter, a variable coding rule is employed for embedding secret bits and decreasing the length of the code stream carrying the secret bits. Unlike conventional VQ-compression, the scheme of Wang et al. can reduce the output code-stream size by 10% on average, and the associated average hiding capacity per test image is approximately 30,000 bits. Reference [7] is the most recent published paper by using VQ to hide data. It presents image watermarking method based on classified VQ. Each block is encoded by the classified VQ codebook according to its class and the two watermark bits corresponding codebook. This scheme is a blind watermarking method and the watermarked image is robust to most of common signal processing operations. In this paper, we present a novel watermarking scheme for hiding the bi-level, gray-level, color, and text watermarks.

### II. PROPOSED METHOD

In this paper, both data hiding (watermark embedding) and retrieval are achieved by vector quantization. However, the time for VQ is quite long which make it an unpractical method in real world. Therefore, we adopt two processes to speed up VQ. The factor to spend time to fulfill VQ is the searching area. Conventional VQ encoder searches the whole codebook for every input vector to find the best match codeword. In this paper, we limit the searching area by calculating the codewords whose average values are close to the input vector. For the image (I) used to hide data, it would be divided into non-overlapped sub-blocks  $x=(x_1, x_2, x_3,...,x_k)$  whose size is n by n and  $k=n\times n$ . The average of x can be got by

$$\overline{\chi} = \frac{\sum_{i=1}^{k} x_i}{\nu} \tag{4}$$

Meanwhile, we also need an extra space  $\overline{Y}$  to store the sorted average value of each codeword in codebook Y whose size is N according to

$$\overline{y_j} = \frac{\sum_{i=1}^k y_{j_i}}{k}$$

$$j = I..N.$$
(5)

For every sub-block x, we search the codewords whose  $|\overline{x} - \overline{y_j}| \le \partial$  to find the best match codeword. If there are M codewords  $\{y_1^{\varphi}...y_M^{\varphi}\}$  that meet the condition above in Y, we will use the following method to decrease the computation

burden furthermore. Basically, the main idea is to decrease the computation in (1). Partial distortion searching (PDS) algorithm can be used to accelerate the computation. In PDS, the calculation of searching can be terminated once the accumulated partial error exceeds the current minimum total error during the calculation of (1).

The algorithm of PDS is summarized as:

From the PDS pseudo codes, it can be observed that the encoder can decide that a codeword is inappropriate before finishing the computation of the distortion for a codeword by the virtue of premature exit. This occurs when the accumulated distortion  $d_{cur}$  for the first j pixels of the input vector is larger than the smallest distortion already found in the searching of  $d_{min}$ . Refer to the loop A in Step 2, which ensures that we only search the partial of the whole codebook. It is un-necessary to search the entire codebook. In this paper, we limit the searching range according the criteria in the previous section. In addition, the PDS can save a lot of computation burden as well. Notice that no matter data hiding or data retrieval from the image in this paper, both of them are fulfilled by the VQ. Therefore, fast VQ can save a lot of time for both hiding and retrieval. In real application, fast VQ costs about 2.5% time compared to conventional VO in embedding or retrieval watermark. Experimental results show that the embedding time is less than 0.5 seconds.

In the research field of data compression for VQ, conventional method to yield codebook is by LBG [2]. The time to generate codebook is long; however, the codebook is global that means once it is yielded, the codebook will be used by all the images. In this paper, we need to yield the twin-codebook to embed the watermark. Every codeword' size is  $4 \times 4$  in the codebook Y. We generate another codebook Y and the codeword size in Y' is  $4 \times 4$  as well. The size N of the whole codebook of Y and Y' is the same. However, the content of  $y_i$  and  $y_i'$  ( $1 \le i \le N$ ) has tiny difference by modifying the codeword content in  $y_i$  to another value in  $y_i'$ . We first re-arrange the  $4 \times 4$  codewords into one-dimension array whose size is  $16 \cdot y_i$  is the codeword in original codebook  $(Y) \cdot y_i'$  is the twin codeword for  $y_i$ . Notice that the number, location and value of the elements to be modified are randomly yielded.

The algorithm to yield the twin-codeword from  $y_i$  to  $y_i$ ' is given as:

/\* decide the number of pixel to be modified \*/
Step 2: for (a=0; a<#number; a++)
{
 location= rand()%16; (9)

/\* decide the location to be modified \*/  $y'_{location} = y_{location} + (rand()\%10) - 5;$ (10)

/\* modify the value \*/
 while ( $(y'_{i_{location}} \ge 255)$  or ( $y'_{i_{location}} \le 0$ ))
/\* boundary check of bit depth \*/  $y'_{i_{location}} = y_{i_{location}} + (rand()\%10) - 5;$ } (11)

Notice that we limit the number of content modification to 8 at most and the pixel deviation between yi yi' is  $-5 \sim +4$ . In addition, the value modification will be constrained to the bit depth range. That is because we don't want to cause apparent visual difference for the twin codewords to avoid unpleasant visual effect after embedding watermark. The following is an instance whose #number =4 and the locations will be modified are 5,8,11,16. You can observe the value modification from the black number to red number by the arrow sign.

$$y_i = [65,54,34,125,21,52,123,135,54,213,212,123,214,58,120,93]$$
  
 $y_i' = [65,54,34,125,23,52,123,132,54,213,207,123,214,58,120,97]$ 

The amount of data hiding is determined by the size of image and codeword. Assume the gray image size is  $A \times B$  and the size of each codeword is  $4 \times 4$ , the capacity that can hide data is  $(A \times B)/(4 \times 4)$  bits. From the aspect of data compression, we know that image is compressed by VQ encoder and de-compression on decoder. The watermark embedding process is achieved during the encoding and decoding. After this embedded process, we can say that the data is hided in this image. Fig. 2 depicts how the embedding job works. For every sub-block in the original image (I), we must find out the ymin from Codebook I. However, the codewords selected to paste on the embedded image ( $\bar{I}$ ) are determined by the watermark data. If the data to hide is '0', we paste the codeword whose index is  $y_{min}$ ; otherwise, we paste the codeword whose index is  $y'_{min}$  to the embedded image. Notice that the searching process is fulfilled to the Codebook I only for every input vector x and the difference between the twin-codebook and twin-codeword is tiny which is almost visual indistinguishable. VO will cause the distortion when the codebook size is small to achieve higher compression ratio. In this paper, compression is not the goal so that we increase the codebook size to decrease visual distortion.

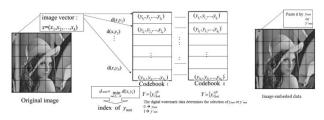


Fig. 2 Configuration for embedding and retrieval

The operation of data retrieval from the embedded image is quite simple, we search both Codebook I and Codebook II to find the best matched codeword for every sub-block in ( $\bar{1}$ ). If the searched codeword is belonged in Codebook I, we can output the value of '0'; otherwise, output '1'. By this manner, we can output the whole watermark.

Embedding the watermark is to protect the property of owner or hiding the data. In addition, we have another processing to protect the watermark furthermore by confusing it. Here, bi-jective mapping function is adopt to make the watermark being confused. Original watermark will become very difficult to understand or recognizable. It is very difficult to recover the original watermark without the key of the function. The bi-jective mapping function is given as:

$$F(p) = (A + B \times p)MOD M \tag{12}$$

Here, A and B are private keys and M is the total data amount. B and M must be coprime. p is the original position. F(p) will yield the new position. Fig. 3 shows a watermark is confused by the above function.

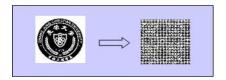


Fig. 3 Confusion of watermark

In this paper, the data to hide could be one of the following four forms as bi-level, gray, color images and text. Image data must be converted into a binary stream composed by 0 and 1. Bi-level image is very easy to process because it is binary form. For 8 bit-depth gray image data, we must convert a gray pixel value into binary form. There are Red, Green and Blue three spaces for each color pixel so that it is necessary to converting each space into binary before embedding. As to the text, we can use Chinese, English with punctuation to be the watermark. ASCII codes are used to represent these texts. ASCII codes can be converted into binary codes to embed. Fig. 4 shows the original image after VQ and the image embedded with watermark.





Fig. 4 (a) Without embedded data (b) With the embedded data

In order to increase the privacy of the method, we store some parameters to be the key  $(\pounds)$  to retrieval the watermark. The parameters are composed as (watermark\_length, watermark\_width, watermark\_type, A, B). A and B are the parameters in bj-jective mapping function. Embedding watermark is achieved by twin-codebook and yield embedded image  $(\overline{I})$  and key  $(\pounds)$ . By using the twin-codebook and  $\pounds$ , we can retrieval the watermark from the embedded image  $(\overline{I})$ .

The quality of the system performance can be evaluated by following factors: a. speed b. subjective observation for image-based type watermark. c. objective measurement in terms of mathematic calculation. d. correctness percentage of text. Mathematic evaluation can be achieved by mean square error (MSE) as:

$$MSE = \frac{1}{r \times s} \sum_{i=1}^{r} \sum_{j=1}^{s} (w_{ij} - \overline{w}_{ij})^{2}$$
 (13)

r and s are the size of the size of image-based watermark.  $w_{ij}$  is the original watermark and  $\overline{w}_{ij}$  is the retrieved watermark. If the watermark is color, we get the average MSE value from the R G B three planes.

## III. EXPERIMENTAL RESULTS

The size of the twin-codebook we use in the experiment is 1024. Notice that the image we embedding is color image. Therefore, we yield three twin-codebooks for R, G, B by LBG algorithm, respectively. The image size is 512×512, sub-block size is 4×4, the total of amount data capacity to hide the watermark is 49,152 bits. With the aid of fast-VQ, the embedding time is less than 0.5 seconds. Embedding time is half compared the retrieval time because that we only search codebook I in embedding and search codebook I and codebook II in retrieval.

In order to evaluate the robustness of the data hiding performance, we embed the four forms of watermarks as mentioned in the previous section and using tools in Photoshop to modify the content the embedded image to test the robustness of the system. If there is no modification imposed on the embedded image, the retrieved watermark is 100% the same as the original watermark. The image processing operations we use for robust testing are sharpness, hollow out, adding the text to the embedded image. You can observe the performance from Figs. 5-8.



Fig. 5 Embedding bi-level watermark

Fig. 6 Embedding gray watermark

a. Embedded Image	b.	Retrieved Watermark
c. Sharped Embedded Image	d.	Retrieved Watermark (MSE=1899)
e. More Sharped Embedded	f.	Retrieved Watermark (MSE=9386)
Image		
g. Embedded Image (hollowed)	h.	Retrieved Watermark (MSE=4598)
		(1.052 1.050)
i. Embedded Image (hollowed)	j.	Retrieved Watermark (MSE=77310)
k. Embedded Image (Addition texts)	1.	Retrieved Watermark (MSE=5795)
長榮大學		(NOL - 7/73)

Fig. 7 Embedding color watermark

Figs. 5-7 show that the experimental results of retrieved watermarks at different alternations to see the robustness of the data hiding system. The logos are all almost recognizable in

Figs. 5-7 except the case in Figs. 5-i, 6-i and 7-i. In those cases, the hollowed area exceeds more than half of the embedded image.

image.	
a. Embedded Image	b. Retrieved Watermark (total=223)
	政府主持大人。 以
c. Sharped Embedded Image	d. Retrieved Watermark (error=91)
	政府重□開疾美讚帶骨拍肋 進□高雄俗長陳蘭今妩10股 26懿 表陳蘭及國調評令 東京 在 東京 在 東京 在 東京 在 東京 在 東京 在 東京 在 東京 在
e. More Sharped Embedded Image	f. Retrieved Watermark (error=171)
	極□郵□鶉吘美讚、騠籅庫 2・ 善高雄俗侵陳拉캊天¬11 最2□淳(∴示,炖◆房看警据 康烈中央 立・愈針新蛇佰 設 頑支壊%罩涨針者>>> 「被違潛 陳溫豨砻、經過淶合加工绌掌 絞肉等辨莊龐離劘也難大 、・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・



(error=102)



麵待重新鞋鏈"國帶誨牛肉録 立高雄市長陣菊今天h10柴 2日臟顨示,為飧及國亪偭 介,中儮主管櫿闌·重新詍鑷 這項捨楞弌給消費者離個喉 風、安心<br/>
は消費環墁nA 療・衠慎,經過海合加◆皔・ 絞肉等莨莊困難**令**也難以追 查掯管, 崴須從伤源加勡管娶 あ陳局說,台笏布政府推凸胪 主管到世農,與高黄市政府· 前因凉〈鸚殺氯腺事件」籔授 煉炀台瀣產品專印佄法鋷 同,陳莉認犹,渭央为管機團 應遍蹤• 如瞌國帶蚲牟肉進口 政策, 逌%是讓匰方朿府執行 一項 艦共政策璸抗蠡的樑尪 · 增加焥謃的行+成本。

Fig. 8 Embedding Traditional Chinese text watermark

The experimental results in Fig. 8 is different to others, text watermark is different to the other types of watermark. Any modification imposed on the embedded image will cause the changing of the hidden text. The correction rate should be 100% in case the misunderstanding. There is another alternative method to improve this kind of defect by transform the text into image format watermark. From the observation of the above experiments, we know that the image watermark is more robust than text watermark. Text watermark is fragile while attacking the embedded image.

### IV. CONCLUSION

In this paper, the data hiding method is proposed by VQ encoding and decoding to the image. VQ distorts image essentially. However, if the codebook size is large enough such a distortion is tiny in visual sense. But, big codebook size will take too much time while embedding or retrieving the watermark. Thus, we adopt big size codebook and fast VQ encoding method to speed up the processing time while maintaining image quality so that the user will not perceive the image is embedded data. There are twin codebooks in this paper. Watermark being embedded is spread to a chaotic pattern and transformed into binary data. By way of selecting from the twin codewords, binary data is hidden in the image. The proposed is reversible watermarking scheme when the embedded image is not alternated. The experimental results demonstrate that the proposed method is robust to most of common signal processing imposed on the embedded image.

#### REFERENCES

- Y. Linde, A. Buzo, R. Gray "An algorithm for vector quantizer design" IEEE Trans. Commun., 28, 1980,pp. 84–95.
- [2] N.M. Nasrabadi, R. King 'Image coding using vector quantization: a review" IEEE Trans. Commun., 36 (8) ,1988, pp. 957–971.
- [3] Y.C. Lin, C.C. Wang, "Digital images watermarking by vector quantization" *Proc. Natl. Comput. Symp*, 1999,pp. 76–87.
- [4] B. Yang, Z.M. Lu, S.H. Sun, Reversible watermarking in the VQ-compressed domain, in: Proceedings of 5th IASTED International Conference on Visualization, Imaging and Image Processing, 2005, pp. 298–303.

## International Journal of Information, Control and Computer Sciences

ISSN: 2517-9942 Vol:9, No:5, 2015

- [5] C.C. Lin, S.C. Chen, N.L. Hsueh "Adaptive embedding techniques for VQ-compressed images" Inform. Sci., 179 (3) 2009, pp. 140–149.
  [6] L. Wang, Z. Pan, X. Ma, S. Hu "A novel high-performance reversible data hiding scheme using SMVQ and improved locally adaptive coding method' J. Vis. Commun. Image Represent., 25 (2) ,2014, pp. 454–465
  [7] Xu Ding, Zhe-Ming Lu and Fa-Xin Yu" A Robust Blind Image Watermarking Scheme Based on Classified Vector Quantization ", Journal of Information Hiding and Multimedia Signal Processing
- Journal of Information Hiding and Multimedia Signal Processing, Volume 6, Number 1, January 2015.