International Journal of Image Processing Techniques – IJIPT
Volume 1 : Issue 1
Publication Date : 09 January 2014

Reversible Image Authentication Scheme for VQ Images Using Codebook Clustering

Jun-Chou Chuang, Pei-Yu Lin

***Abstract*—The paper presented a reversible image authentication scheme for VQ images using codebook clustering. The proposed method not only locates the alterations of VQ images but also recover the indexes of VQ image without any distortion from the marked VQ indexes after the hidden authentication bits have been extracted. The method uses the codebook clustering to generate four fixed-size small codebooks. Those small codebooks were used to encode original image to obtain a watermarked VQ image. The proposed method has two advantages. Firstly, the hidden procedure of the proposed method is the same as VQ encoding. After the image is finished encoded, the watermarked image is generated. Secondly, the proposed method does not cause any distortion of indexes of VQ image after we extract the hidden data from the watermarked VQ image.**

Keywords—Reversible data hiding, VQ image authentication, digital watermarking, codebook clustering

I. Introduction

As the computer technology, a large amount of digital contents such as text, graphics, video, and audio were distributed on the Internet. However, digital data is very ease to be modified and copied on the open environment. Therefore, it is very important to protect the security during data transmission. The most common used encryption schemes are DES and RSA. The cryptography obtains good security, but increasing more computation complexity.

Image-hiding schemes embed secret data into the cover images in order to provide secure channel for data transmission undetectably. Image hiding schemes are either reversible or irreversible. Irreversible image hiding schemes modified cover images directly, and they do not have the capacity to recover the original image after extraction of the embedded data. As a result, the recover capability is essential and required for lossless cover images embedding such as valuable images, medical images, and military images.

Two well-know reversible image hiding schemes in the uncompressed domain are difference expansion [7] and histogram shifting [5]. Difference expansion scheme first calculates the difference and average values of two neighboring pixels. The difference value is first multiplied by 2 and then the secret bit is appended into the least significant bit of the shifted difference value. Histogram shifting scheme modifies pairs of peak and zero values from the histogram of the cover image to conceal the secret data into the cover image.

Currently, reversible image hiding schemes in the compression domain have been popular discussed. In typically, digital images in the compressed formats can decrease the storage size and shorter the transmission time. Many researches attempted to hide the confidential data in a vector quantization (VQ) compressed image [3, 4] with reversible capability. Reversible VQ-based image hiding has ability to recover original VQ indexes after extraction the embedded secret data.

In 2008, Chang et al. [1] proposed a VQ-based image authentication by codebook clustering. The method uses codebook clustering to divide a codebook into two equal-sized sub-codebooks. One of the sub-codebook is used to hide watermarking bit 1, and the other is used to hide watermarking bit 0. In 2010, Shen and Ren [6] proposed a robust associative watermarking technique based on vector quantization. The method applied the associative rules to combine the image features along with the VQ indexes. Chuang and Hu [2] proposed an adaptive image authentication scheme for VQ image. The method adaptive embeds the watermarking bits into the selected VQ indexes by the module operation. In view of the above VQ-based image authentication schemes are irreversible; therefore, we would propose a reversible image authentication scheme for VQ images using codebook clustering.

The method uses clustering to train an original VQ codebook into two sub-codebooks called sub-codebook G_0 and sub-codebook G_1. The sub-codebook G_0 and the sub-codebook G_1 were used to hide authentication bits 0 and 1, respectively. In order to achieve data reversibility, the sub-codebook was further clustered into the encoding codebook and the recover codebook. The input image block is to search the closest codeword from the encoding codebook from sub-codebooks G_0 and G_1. The encoding codebook in the sub -codebooks G_0 and G_1 was used to encode the input image block. The recover codebook in the sub-codebooks G_0 and G_1 was used to recover the original VQ index. After all image blocks were finished encoded, a watermarked VQ image is obtained.

Jun-Chou Chuang
Computer Science and Communication Engineering, Providence University, Taichung 43301, Taiwan.
E-mail: lzchung@pu.edu.tw

Pei-Yu Lin
Information Communication, Yuan Ze University,
Chung-Li 32003, Taiwan.
E-mail: pylin@saturn.yzu.edu.tw

The rest of this paper is organized as follows. In Section 2, we would review the vector quantization, the pair-wise nearest clustering embedding scheme, and Chang-Chuang-Wang's image authentication method. In Section 3, we introduce our proposed method. In Sections 4 and 5 include experimental results and discussions.

II. Related Work

In this section, we would review VQ encoding/decoding, the pair-wise nearest clustering embedding scheme, and the Chang-Chuang-Wang's image authentication method.

A. *Vector Quantization*

Vector quantization (VQ) is a palette-based lossy image compression scheme, and it consists of three main parts, codebook generation, encoding, and decoding. A well codebook design impacts on image quality of VQ decoding image. The LBG algorithm is a well-know codebook generation technique which was proposed by the Line, Buzo, and Gray. The LBG method uses vector clustering to generate N representative codewords.

In VQ encoding, the input image block is to search the closest codeword in the codebook by the Euclidean distance. The codeword has the minimal error distortion to the input block would be selected to record. That is, an image block with k-dimensional Euclidean space R^k is mapping to a finite subset $CB=\{cw_i \mid i= 0, 2, \ldots, (N\text{-}1)\}$, where CB denotes the codebook with N codewords, and cw_i denotes the i-th codeword in the codebook. In the VQ decoding procedure, each input VQ index searches the original codebook by the table lookup operation to reconstruct image. The diagram of VQ encoding and decoding is shown in Fig. 1.

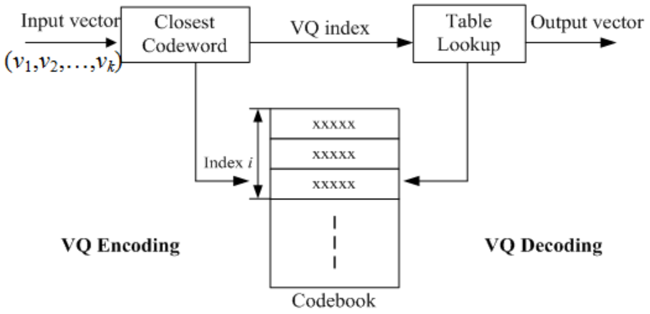


Figure 1. The VQ encoding and decoding diagram

B. *The Pair-wise Nearest Clustering Embedding*

In 1999, Lin and Wang [3] proposed pair-wise nearest clustering embedding (PNCE) method for VQ image hiding. The PNCE scheme selects the closest pair from the original codebook at each time. The result of PNCE partitioned a codebook into two equal-size sub-codebooks. An example of PNCE is shown in Fig 2.

In Lin and Wang's method, the sub-codebook g_0 is used to hide secret bit "0" and the other sub-codebook g_1 is indicated to hide secret bit "1". Each closest pair of codewords in sub-codebook g_0 and g_1 is similar to each other. Thus, the replacement with the alternative matching codeword does not cause serious distortion of reconstruction image.

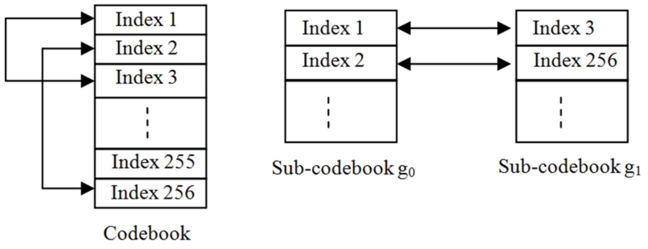


Figure 2. An example of the PNCE method

C. *Chang-Chuang-Wang's method*

In 2008, Chang et al. proposed an image authentication scheme [1] for VQ images using codebook clustering. In their method, they first divided an original VQ codebook into two equal-sized sub-codebooks CB_0 and CB_1. The sub-codebook CB_0 is to hide authentication bit 0. As to the sub-codebook CB_1 is to hide authentication bit 1. The host image was first divided into many non-overlapping macro blocks and each macro block contains 16×16 pixels. After that, each block is further divided into (16/4)×(16/4)=16 sub-blocks. A sub-block embeds only one authentication bit by referring the sub-codebooks CB_0 and CB_1. If one of a sub-block is been tampered with then a macro block is said tampered with. The diagram of the method is shown in Fig. 3.

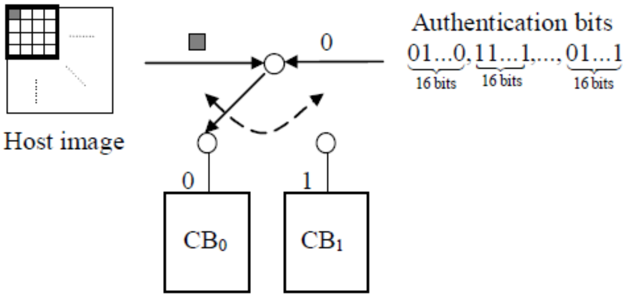

Authentication bits
$\underbrace{01\ldots0}_{16\text{ bits}},\underbrace{11\ldots1}_{16\text{ bits}},\ldots,\underbrace{01\ldots1}_{16\text{ bits}}$
Host image
0
0
1
CB_0
CB_1

Figure 3. Chang-Chuang-Wang's method [1]

III. The Proposed Scheme

Chang-Chuang-Wang's image authentication method is irreversible embedding. The goal of our proposed method would propose a reversible embedding for VQ image authentication. The proposed method not only locates the alterations of VQ images but also recover the indexes of VQ image without any distortion from the marked VQ indexes after the hidden authentication bits have been extracted.

The proposed scheme contains three parts. The first part is the two-stages codebook clustering. The second part is the embedding procedure. The last part contains authentication procedure and recovery procedure. The details of our proposed scheme are described as bellows.

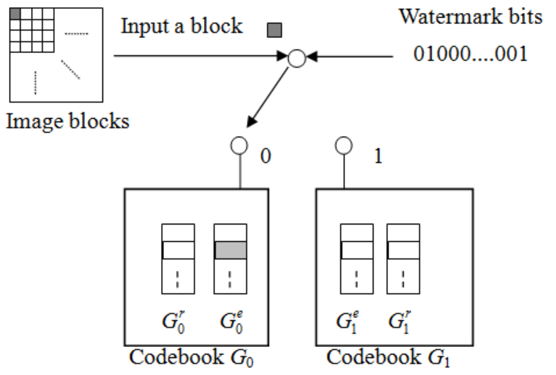


Figure 4. The embedding diagram of the proposed scheme

The embedding diagram of our method is shown in Fig. 4. The proposed scheme applied the concept of PNCE clustering to train an original VQ codebook into two sub-codebooks in equal size, namely, sub-codebook G_0 and sub-codebook G_1. Sub-codebook G_0 is used to hide authentication bit 0, and sub-codebook G_1 is used to hide authentication bit 1. An example of the first stage codebook clustering by the PNCE is shown in Fig. 5.

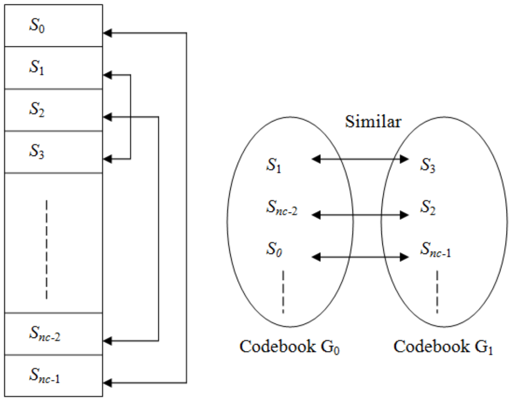


Figure 5: An example of the first stage codebook clustering

In order to archive the reversibility, each sub-codebook is further clustered into the encoding codebook and the recover codebook by the PNCE method. We illustrated an example in Fig. 6 to show the encoding codebook and recover codebook. Each closest pair of codeword in the encoding codebook and recover codebook is similar to each other. Because of the VQ index in the encoding codebook is similar to its corresponding VQ index in the recover codebook. Thus, the image quality would not cause serious distortion.

Firstly, our method was applied encoding codebook in G_0 and G_1 to encode each input block of 4×4 pixels. Secondly, each VQ index was embedded one authentication bit. As we mention above, the VQ index in the sub-codebook G_0 is used to hide authentication bit 0, and the VQ index in the sub-codebook G_1 is used to hide authentication bit 1.

Assume we want to embed a watermarking bit w=1. If a VQ index s_j is belonged to sub-codebook G_0, then we should find its corresponding matching VQ index s_t from the recover codebook G_0^r.

The embedding rules were listed below.

Rule1: If (w=0 and $s_j \in$ G0), then no change s_j.

Rule2: If (w=1 and $s_j \in$ G0), then replaced s_j with s_i in G_0^r

Rule3: If (w=0 and $s_k \in$ G1), then replaced s_k with s_t in G_1^r

Rule4: If (w=1 and $s_k \in$ G1), then no change s_k.

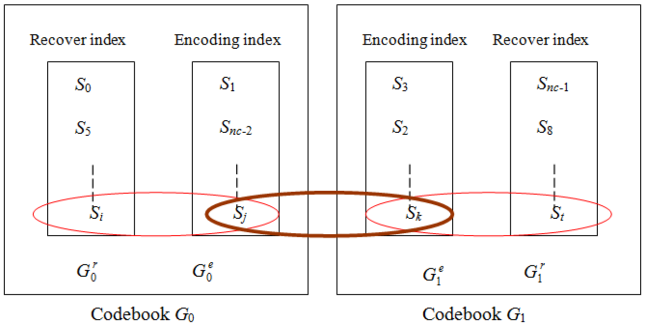
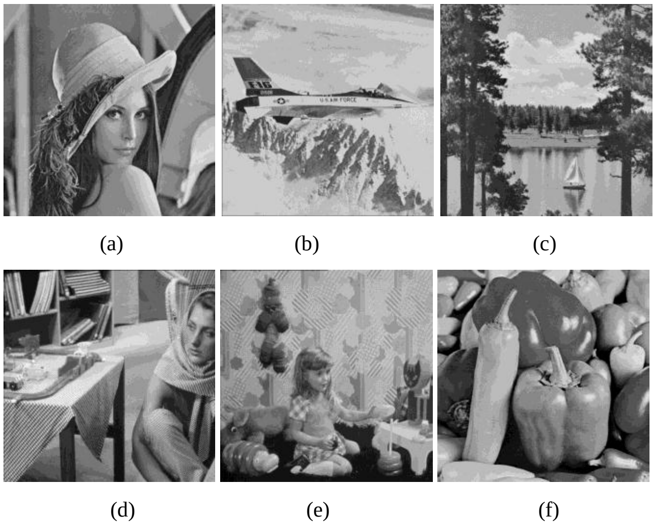


Figure 6. The encoding codebook and recover codebook

In the authentication and recovery procedure, we first extract the embedded data from watermarked VQ indexes. A block is said been tampered with only if the extracted watermarked bit is not the same to original one. On the other hand, a VQ index fallen to the recover codebook is change to it corresponding VQ index in encoding codebook.

IV. EXPERIMENTAL RESULTS

Several experiments were made in image quality and tampering detection. Six 512×512 grayscale images, called "Lena", "F-16", "Boat", "Barbara", "Girl", and "Peppers", were used as test images and shown in Fig. 7. The first five images were used as the training images, and the image "Peppers" was the outside image. The codebook sizes in our experiments were 512, 1024, and 2048.


(a) (b) (c)

(d) (e) (f)

Figure 7: The six test images

The tampered image and detected image were shown in Fig. 8. Fig. 8(a) shows the watermarked image "Lena" where we added one eye on the shoulder. The detected image was shown in Fig. 8(b). The black color indicates that the part has been tampered with.

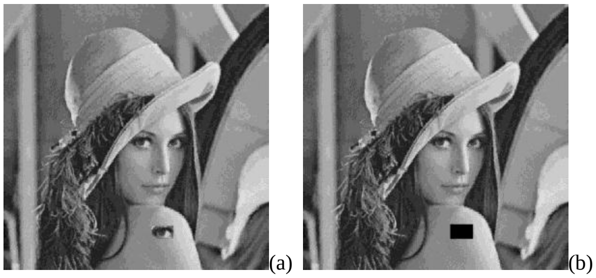
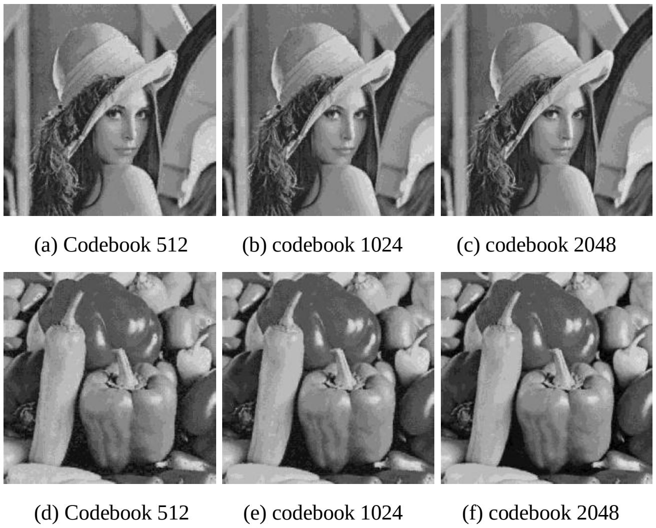


Figure 8: Verification result (a) Tampered image (b) Detected image

The visual quality of watermarked images “Lena” and “Peppers” by using different codebook size 512, 1024, and 2048 were shown in Fig. 9. The peak signal to noise rate (PSNR) of VQ images and watermarked VQ images at different codebook size 512, 1024, and 2048 were listed in Table 1. A large codebook decreases the distortion of recovered VQ images, but increasing the storage size of VQ index.


(a) Codebook 512 (b) codebook 1024 (c) codebook 2048

(d) Codebook 512 (e) codebook 1024 (f) codebook 2048

Figure 9: The watermarked images

TABLE 1. The PSNR values of VQ images and watermarked images at different codebook size 512, 1024, 2048

		Lena	F-16	Boat	Barb	Girl	Peppers
Original VQ	512	31.97	30.72	28.92	26.63	32.25	28.68
	1024	32.64	32.27	29.63	27.50	33.35	29.17
	2048	33.32	33.19	30.62	29.03	34.46	30.16
Watermarked VQ	512	28.42	27.39	26.18	23.06	28.50	27.34
	1024	29.52	28.52	26.93	24.76	29.49	28.44
	2048	30.51	29.83	27.87	25.61	30.89	29.86

V. Conclusion

In this paper, we have proposed a reversible image authentication for VQ images by using codebook clustering. The original VQ codebook is divided into two equal-sized sub-codebooks, sub-codebook G_0 and sub-codebook G_1. The sub-codebook G_0 is to encode authentication bit 0, and the sub-codebook G_1 is used to encode the authentication bit 1. Besides, the sub-codebooks G_0 and G_1 were further divided into two kinds of codebooks, encoding codebook and recover codebook. The encoding codebook in the sub-codebooks G_0 and G_1 was used to encode the input image block. The recover codebook in the sub-codebooks G_0 and G_1 was used to recover the original VQ index. After all image blocks were finished encoded, a watermarked VQ image is obtained. From the experimental results show that the proposed method can obtain acceptable image quality of watermarked VQ image. Besides, our method does not cause any distortion of VQ indexes after we extract the hidden data from the marked VQ indexes.

Acknowledgment

The authors gratefully acknowledge the support provided to this study by the National Science Council of Taiwan under grant number NSC 101-2221-E-126-008.

References

[1] C. C. Chang, J. C. Chuang, and Y. Z. Wang, "VQ-based oriented image tamper proofing schemes for digital grayscale images," *Intelligent Information Hiding and Multimedia Signal Processing* (IITA2008), Shanghai, China, Vol. 1297-1300, 2008.

[2] J. C. Chuang and Y. C. Hu, "An adaptive image authentication scheme for vector quantization compressed image," *Journal of Visual Communication and Image Representation*, Vol. 22, No. 5, pp. 440-449, 2011.

[3] Y. C. Lin and C. C. Wang, "Digital images watermarking by vector quantization," *Proceedings of National Computer Symposium*, Vol. 3, pp. 76-87, 1999.

[4] Y. Linde, A. Buzo, and R. M. Gary, "An algorithm for vector quantization design," *IEEE Transactions on Communications*, Vol. 28, No. 4, pp. 84-95, 1980.

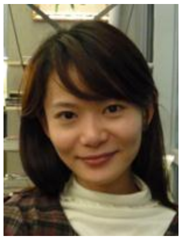
[5] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, pp. 354-362, 2006.

[6] J. J. Shen and J. M. Ren, "A robust associative watermarking technique based on vector quantization," *Digital Signal Processing*, Vol. 20, pp. 1408-1423, 2010.

[7] J. Tian, "Reversible data embedding using difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 890 -896, 2003.

About Author (s):

	Jun-Chou Chuang is an associative professor in the Department of Computer Science and Communication Engineering, Providence University, Taiwan. His research interests include multimedia, data hiding, digital watermarking, and signal processing.

	*Pei-Yu Lin* is an assistant professor in the Department of Information Communication, Yuan Ze University, Taiwan. Her research interests include multimedia security, data hiding and digital watermarking.