Experimental Analysis of an Optimized Watermarking Scheme Based on Convolutional Coding Techniques*

ZOU Yan, LU Pei-zhong
(Department of Computer Science and Engineering, Fudan University, Shanghai 200433, China)

Abstract: This paper presents a detailed experimental analysis of a DCT-domain watermarking scheme based on convolutional coding techniques. Our results show that choosing suitable convolutional code can considerably alleviate the trade-off between the capacity and the robustness against most of attacks.

Key words: watermark; convolutional code; viterbi decoding
CLC number: TP391.4 **Document code**: A **Article ID**: 0529-6579 (2004) S2-0143-05

Digital watermarking has emerged as an appropriate tool for copyright protection. There is a trade-off between the capacity and the robustness of the watermarking system. Some researchers applied error correction codes (ECC) in watermarking system. R. Hernández and his colleagues propose a convolutional code watermarking scheme to improve the performance of data hiding in spatial domain[1]. Their experimental results show that their method performs better than the uncoded one and other error correction code ones. But their experiments are not sufficient to analyze the robustness against attacks such as additive noise, cropping etc. And they don't measure the capacity of their scheme explicitly.

In this paper, we first make a further investigation of Hernandez's scheme in [2]. Then we modify their scheme by using convolutional codes to obtain an optimized watermarking system that performs much better on capacity and robustness. We apply Viterbi soft-decision for decoding and achieve better detection performance. A major part of our work is to investigate how the application of convolutional codes affects the capacity and the robustness. Ramkumar[3] presents an information-theoretic approach to estimate the capacity of still images. We perform the same experiments to compare with it using our watermarking scheme. The results show that the gains of convolutional codes used in our watermark scheme are very remarkable. We can see that even surviving the low-quality JPEG compression, our scheme still has large capacity. In addition, the experimental results also show that our scheme can resist Gaussian noise and cutting or scrapping efficiently.

1 Watermarking Scheme

1.1 Embedding Algorithm

The watermark embedding algorithm is roughly shown in Fig. 1. The letterdenotes the 2—D pixel matrix consisting of elements $x(i, j)$, $0 \leqslant i < L_1$, $0 \leqslant j < L_2$, where L_1 and L_2 are the width and height of the original image. First, we perform DCT on the original

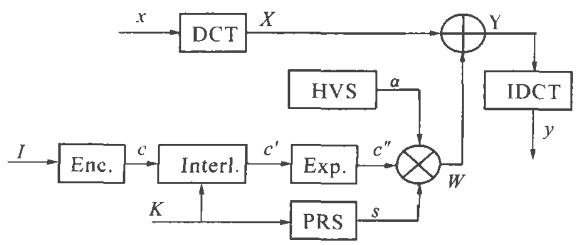

Fig. 1 Watermark embedding process

image x and obtain the DCT coefficients X. The Information I that will be hidden in the original image is a bit sequence with length of N_b. After convolutional encoding we obtain a N_c bits codeword vector $c = (c_1, c_2, K, c_{N_c})$. For security purposes, the codeword is passed through an interleaver and the output is $c' = (c'_1, c'_2, K, c'_{N_c})$. Then the codeword c' is expanded into a 2—D signal by means of a replication process in each different set S_i, $i \in \{1, \cdots, N_c\}$. After the expansion process a 2—D sequence is generated with the same size as the original image. Then the watermark is obtained:

* 收稿日期: 2004—09—10
基金项目: 国家自然科学基金资助项目 (10171017, 90204013); 上海科学技术基金资助项目 (035115019)
作者简介: 邹艳 (1978 年生), 女, 博士生; E-mail: 031021075@fudan.edu.cn

$$W = c'' \circ s \circ \alpha \qquad (1)$$

Where s is the output of a PRS generator with an initial state, which depends on the value of the secret key K. And α is obtained through a perceptual analysis of the original image. Adding the watermark to the DCT coefficients we obtain:

$$Y = X + W \qquad (2)$$

Finally we perform the inverse discrete cosine transform (IDCT) on Y and get the undistinguished watermarked image in perceptual with the original image.

1.2 Information Extracting Algorithm

We present the information extracting process in Fig. 2. By our method, we do not need the original image for extracting. The watermarked image y' is first decomposed into DCT coefficients Y' by the same transform as in the embedding step.

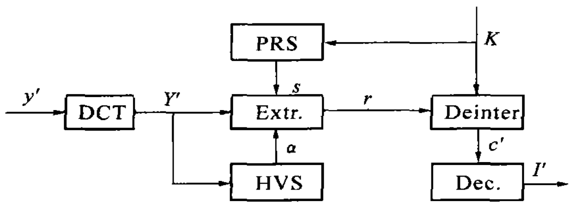

Fig. 2 Information extracting process

In this paper, we use the ML estimate, which is necessary to develop accurate statistic models for the original image. In [2], R. Hernández applies zero-mean generalized Gaussian distributions to statistically model the DCT coefficients of the original image and shows considerable improvements in performance. Here we use the conclusions in [2] for convenient application. By this assumption, the ML estimate of watermark is equivalent to calculate, where $r = \{r_1, \cdots, r_{N_c}\}$

$$r_n = \sum_{S_n} \frac{|Y' + \alpha s|^r + |Y' - \alpha s|^r}{\sigma^r} \qquad (3)$$

Since convolutional code is applied, we decode this soft information by Viterbi soft-decision which is an improvement of the work of Hernández in [2].

3 Convolutional Codes and Soft Decision Decoding

Convolutional encoding with viterbi decoding is an ECC technique that is particularly suited to a channel in which the transmitted signal is corrupted mainly by additive white Gaussian noise (AWGN). Due to the interleaving process and the PRS, the codeword are embedded randomly in different set of the DCT domain. We can infer that all the elements of r have approximately the same mean and variance. Furthermore, if the number of pixels in one set for embedding one bit is large enough, each element of r is approximately the sum of many independent identical variables. Therefore, based on the central limit theorem (CLT) we can assume that the vector r can be accurately modeled as the output of an AWGN channel. Based on this assumption, we can take the advantage of convolutional codes in the watermarking scheme. If the information has the length of $2 \circ L + l$, and the constraint length is l, the output codeword of a 1/2 rate encoder has the length of $2 \circ L + l$. We apply Viterbi soft-decision decoding algorithm, which has the advantage that it has a fixed decoding time. Convolutional codes are more powerful when they are combined with Viterbi soft-decision decoding, which is in fact the optimum ML decoding structure for the AWGN channel[1]. The reasonable constraint length of a convolutional code used in practice is below 10.

3 Experimental Results

In order to assess the improvement in performance by the convolutional codes combined with soft-decision decoding strategy, we perform tests on three standard RGB images with the same size 256×256 pixels: lena, peppers and girls. As we all known, most of the image energy is concentrated in the lower frequency bands in the DCT domain, embedding information in this field may cause distortion. However, embedding information in the higher frequencies in the DCT domain may lose the information because of some compression. At the mid-frequency bands, we could strike a compromise.

3.1 Capacity analysis

By information theory, we know that the capacity of a channel depends on the information signal power and on channel characteristics. For image watermark channel, capacity depends on the watermark strength, on image statistics, and on the way the watermark is embedded[4]. We compare the BER of decoding between the uncoded case and convolutional codes case with respect to the capacity in bits. We choose four different convolutional codes with the same rate 1/2 described in octonary notation: (7, 5), (35, 23), (171, 133), (753, 561), which representing the generator sequence of the encoder. In Fig. 3 and Fig. 4, we show the empirical curves representing the BER as a function of capacity in bits for *Lena* and *Peppers*. From the curves we can see that a severe degradation in BER when using the convolutional codes. And the longer the constraint length is, the better the decoder works. Our scheme achieves higher capacity than that of the uncoded one for a given BER. When BER is kept zero and in the uncoded case, the maximum capacity of these two images is about 300 and 900 bits respectively, corresponding to 0.0046 and 0.014 bits/pixel. However, when the convolutional code (753, 561) is used, the capacity is 1900 and 4000 bits respectively, corresponding to 0.029 and 0.061 bits/pixel.

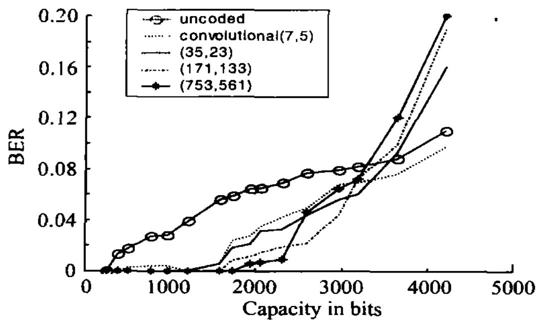

Fig. 3　BER vs. capacity for image Lena

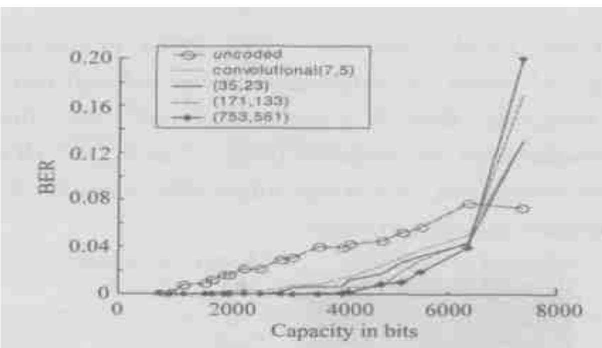

Fig. 4　BER vs. capacity for image Peppers

In [3], Ramkumar presents an information theoretic approach to obtain an estimate of capacity. He models the watermarking system as an additive noise channel and there are two sources of noise: one due to the cover image, the other due to the processing (compression / decompression). When the processing noise is Gaussian and independent of the image noise, the capacity bits can be calculated as:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_s^2}{\sigma_{ig}^2 + \sigma_p^2}\right) \tag{4}$$

Where σ_{ig}^2 is the equivalent Gaussian variance for the image noise, is the variance of the processing noise, andis the message signal energy. For a 256×256 image, assuming that the image noise is uniform distribution and goes through JPEG compression at 50% quality, the capacity is about 140 bits (0.0022 bits/pixel). It is easy to see that our scheme can achieve much higher capacity comparing to Ramkumar's theoretical value.

3.2　Robustness test

Robustness refers to the fact that the embedded information should be reliably decodable after alterations to the watermarked image. In our experiment, we test the robustness in three cases: Gaussian noise, JPEG compression and cutting or scrapping.

3.2.1　Resistance to Gaussian noise

We add different amount of Gaussian noise to the watermarked images which have hidden different capacity of information and we will see the maximum amount of Gaussian noise the images can resist under the constraint that BER is less than 0.01. Fig. 5 plots the curves in the uncoded case and convolutional codes case. From the curves we can conclude that in a certain amount range of noise, the convolutional code scheme shows its better performance on resisting Gaussian noise.

We embed information of 512 bits into image Girls and add different amount of Gaussian noise to the watermarked image. Fig. 6 shows the BER when decoding from these attacked images. The convolutional code scheme works better than the uncoded one when the noise is not severe but the performance declines sharply with the noise is increasing. Generally, the 10% Gaussian noise is so malicious that the image has been destroyed uselessly.

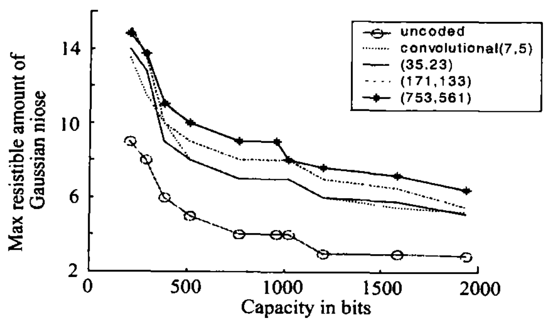

Fig. 5　The max resistible Gaussian noise vs. capacity

3.2.2　Resistance to JPEG compression

We know that JPEG compression is based on removing insignificant components of an image in the DCT domain. Because the watermarks are embedded in the most significant components of the DCT domain, most of the watermark remains unchanged after compressed. So our method in DCT-domain has good performance on resisting JPEG compression, especially in convolutional code cases. The test image is Peppers. First, we perform the JPEG compression with quality factor equal to 10. In Fig. 7 we show the result. Comparing Fig. 4 with Fig. 7, there is nearly no difference between them. That is to say that the influence of the JPEG compression on the performance is very little.

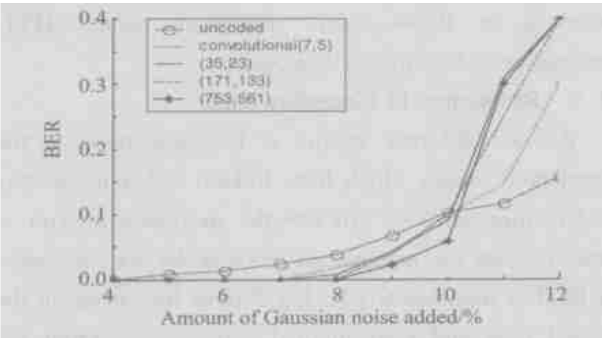

Fig. 6 BER *vs*. amount of Gaussian noise added

In addition, we compare the performance on resisting JPEG compression with the theoretical result in [1]. Ramkumar shows the average capacity estimate for 15 images when the image has to survive JPEG. In Fig. 8 we review his conclusion and we also make a comparison with the empirical results. The bars in Fig. 8 show the max capacity when encountering JPEG compression under the constraint of BER less than 0.01. The index 1 represents the lossless compression. The indices 2～5 correspond to the JPEG compression quality factor 75, 50, 35 and 25 respectively. The theoretical result in this five cases is about 6400, 2400, 1300, 800 and 400 bits respectively. By our method, in the uncoded case the capacity is about 1800, 1600, 1500, 1400 and 1200 bits. There is a little improvement. However, when using convolutional code, for example, in the (753, 561) case, the result is about 5500, 5200, 5000, 4700 and 4600 bits. Though the capacity of our scheme is lower than the theoretical one in the lossless compression case, but it declines very slowly even under low-quality factor JPEG compression.

3.2.3 **Resistance to cutting or scraping**

The attacks of cutting or scraping may cause a severe distortion on the watermarked image. Our experiment proves that our technique can resist such attacks. The test image is Lena; we hide information of 1024 bits in it. We

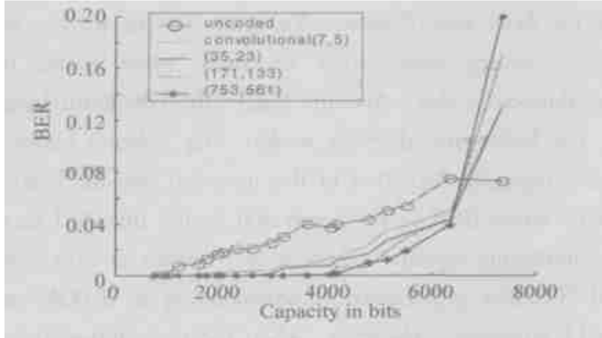

Fig. 7 BER *vs*. capacity suffered JPEG

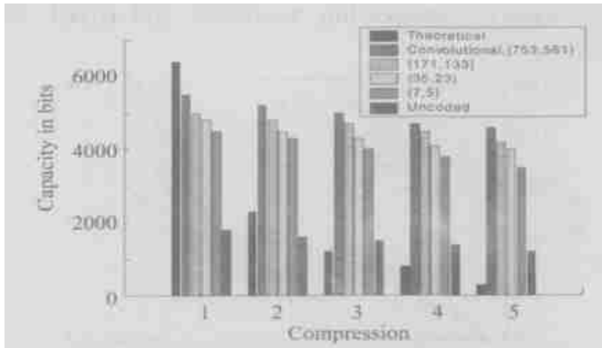

Fig. 8 Capacity comparison when the images survive JPEG compression

apply the convolutional code (753, 561) in the test. Fig. 9 (c) shows the watermarked image suffered cutting and scrapping; there is a severe distortion. We extract information from the attacked image; Fig. 9 (d) shows the recovery result, which has only a little alteration from the original information image.

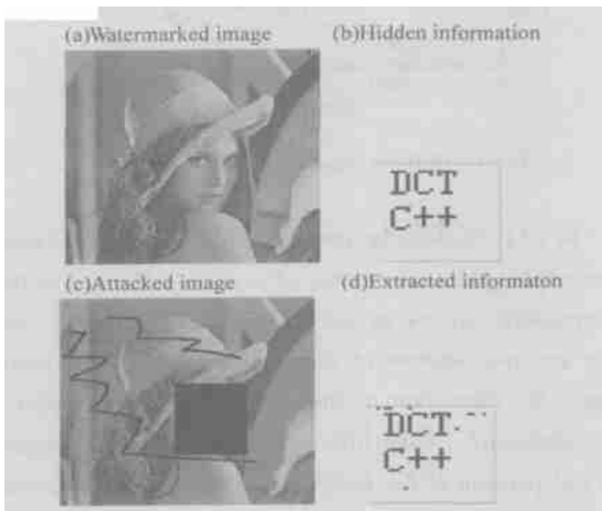

Fig. 9 Resistance to cutting and scrapping for Lena

4 Conclusion

In this paper, we demonstrate the improvement of performance on the DCT-domain watermarking scheme due to the application of convolutional codes and soft-decision decoding techniques. There is a remarkable increase in the capacity comparing to Hernández's scheme[2] and our capacity also exceeds the theoretical value estimated in [1]. The experiments on robustness testing proved that our method has good ability to resist Gaussian noise, JPEG compression and cutting or scrapping. However, our method is sensitive to the attacks that result geometry distortion such as rotation and scaling. We will focus our future work on it.

References:

[1] HERNÁNDEZ J R, DELAIGILE J F, MACQ B. Improving data hiding by using convolutional codes and soft-decision decoding [J]. Security and Watermarking of Multimedia Contents Ⅱ, Proceeding of SPIE, 2000, 3971: 24—47.

[2] HERNÁNDEZ J R, AMADO M, PÉREZ-GONZÁLEZ F. DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure [J]. IEEE Transactions on Image Processing, 2000, 9 (1): 55—68.

[3] RAMKUMAR M, AKANSU A N. Capacity estimates for data hiding in compressed images [J]. IEEE Transactions on Image Processing, 2001, 10 (8): 1252—1263.

[4] VOLOSHYNOVSKIY S, HERRIGEL A, BAUMGAERTNER N, et al. A stochastic approach to content adaptive digital image watermarking [C]. Third International Workshop on Information Hiding, Dresden, Germany, 1999.

结合卷积码技术的优化水印体制的实验分析

邹　艳, 陆佩忠

(复旦大学计算机科学与工程系, 上海 200433)

摘　要: 提出了一种结合卷积码技术的 DCT 域数字图像水印体制, 并给出详细的分析结果。实验表明, 选择合适的卷积码运用于水印体制能缓解水印体制的隐藏容量与鲁棒性之间的矛盾, 并能抵抗大多数恶意攻击。

关键词: 水印; 卷积码; Viterbi 译码

中图分类号: TP391.4