Public Digital Watermark Using Error Correcting Code*

YANG Qing, *CHEN Ke fei*
(Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, China)

Abstract: To propose one publicly detectable watermarking plan using error correcting code. The algorithms for the watermark embedding and extracting are both open, and public key cryptosystem is utilized instead of common watermark key. Anyone can extract and verify the digital watermark embedded in the image, but no one can destroy or alternate the watermark, or retrieve the original image without the corresponding private key. Error correcting code is used to eliminate the negative effect of noise in watermark embedding/extracting and image encryption.

Key words: digital watermark; public key cryptosystem; error correcting code; discrete wavelet transform
CLC number: TP309 **Document code**: A **Article ID**: 0529-6579 (2004) S2-0160-04

1 Introduction

With the rapid development of networking and the wide use of personal computers, people are able to access all kinds of information through digital channels more easily than before. The digital data, such as text, image, video, audio, etc., can be effortlessly retrieved, copied and then stored from the Internet or other digital resources and equipments without the permission of the original authors or copyright owners. This is a big headache for all the innocent manufacturers of digital products, veridical merchants and legal end users. Therefore, data protection and copyright issues are becoming more and more important nowadays. Many researches have been conducted in the field of digital data protection [1], and among them, the digital watermark techniques have attracted most of the researchers' attentions. The word "Watermark" means to embed invisible (or sometimes-visible) or inaudible information into digital data for copyright ownership verification and authentication. In addition to the insensibility requirement, digital watermark should be robust against intentional (i.e. hostile attack) or unintentional (i.e. noise, compression, filtering or other regular processing) watermark removal processing.

For an ideal image watermark, it must satisfy the following requirements:

(1) Imperceptible: The watermark signal must be hidden in the original image and it should not render visible artifact in the original image.

(2) Non-removable: The invisible watermark can't be removed easily without damaging the original image.

(3) Robustness: The watermark should be resistant to the regular image processing, such as lossy image compression (e.g. JPEG), filtering, etc.

(4) Unambiguous: Retrieval of watermark should unambiguously identify the image owner, and the accuracy of identification should degrade gracefully in condition of attacks.

(5) Universal: The watermark technique should be applicable for different kinds of media types, such as image, audio, video, etc.

The watermark techniques can be classified into two major categories based on the casting methods: spatial domain one and transform domain one. Spatial domain watermark is easy to implement and the extracting process can be done without referencing the original image. In spatial domain, the Least Significant Bit (LSB) of the original image is usually replaced by one pseudo random sequence, which can be viewed as the identification. Although it's easy to implement, the watermark will be easily destroyed if the normal signal processing or vicious attacks are applied on the image.

For frequency domain, the basic idea is to modify the coefficients of the image by some certain rule after corresponding transforms, such as DCT, FFT, DWT, etc. After the image is transformed, the watermark signal is embedded into the image in the frequency do main.

In this paper, we propose a public watermark system

* 收稿日期: 2004-08-29
基金项目: 国家自然科学基金资助项目 (90104005); 国家"863"高科技计划资助项目 (2001AA144060)
作者简介: 杨青 (1977 年生), 男, 博士; E-mail: yangqing@sjtu.edu.cn

in discrete wavelet domain. The algorithms for watermark embedding and extracting are both open to the public. And the public key cryptosystem is used instead of common watermark key. Any one can extract and verify the watermark information using the public key, but no one can destroy the watermark or get the original unwatermarked image without the owner's private key. Error correcting codes are used to eliminate the effect of noise and other processing. Through some experiments, we find that this watermark system is of good performance and more practical than other similar systems.

2 The public watermark system

2.1 Basic elements of the system

To perform watermark extracting, the following information is open to the public: watermarked image, public key k_{pub}, watermark embedding function $Em(*)$ and watermark extracting function $Ex(*)$.

For those people who embed the watermark into the image, they should possess the following secret information: original image and private key k_{pvt}.

As we know, public key and private key above are a key pair in general public key cryptosystem[2].

2.2 Watermark embedding and extracting

2.2.1 Watermark embedding procedure

In a public key cryptosystem, public key and private key can be used as encryption key and decryption key alternatively. As to our system, the image is first encrypted with the public key, then the encrypted image is watermarked, and finally the watermarked image is decrypted using the corresponding private key. During the process of image decryption, the watermark information is encrypted at the same time. This is one advantage of the public key cryptosystem[3].

The watermark embedding procedure is shown in Fig. 1.

(1) The original image is transformed by DWT.

(2) Wavelet coefficients of the original image are encrypted with the public key k_{pub}[4].

(3) Using the watermark embedding function $Em(*)$, the watermark is embedded into the encrypted image coefficieots. For image watermark, it should be first quantized before embedding.

(4) The watermarked image is decrypted with the corresponding private key k_{pvt}. Hence, the watermark is encrypted by k_{pvt}.

(5) IDWT is applied on the image coefficients, and the final version of the watermarked image is available.

As we have stated previously, k_{pub} and $Em(*)$ are open to the public, but only those people who possess k_{pvt} can decrypt the encrypted image (also watermarked) to obtain the watermarked image.

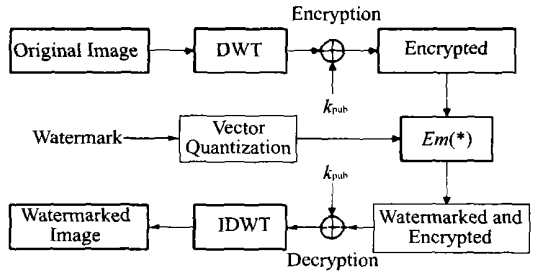

Fig 1　Watermark embedding procedure

2.2.2 Watermark extracting procedure

The watermark extracting procedure is shown in Fig. 2.

(1) The original image is transformed by DWT.

(2) The image coefficients are encrypted with the public key k_{pub}. Hence, the watermark is decrypted.

(3) Using the watermark extracting function $Ex(*)$, the watermark in the encrypted image is extracted. When necessary, source decoding will be performed to get the original image watermark.

(4) IDWT is applied on the image coefficients.

(5) The final result is the encrypted image, and only those who possess k_{pvt} can decrypted it, thus the original image is protected.

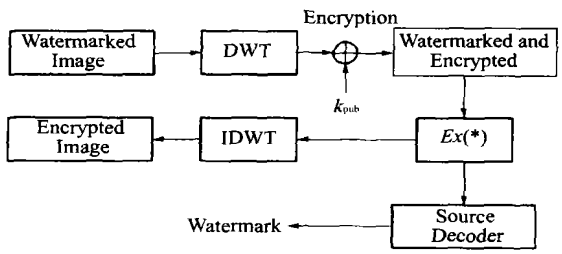

Fig 2　Watermark extracting procedure

In the above procedure, anyone can extract and verify the watermark embedded in the image by the public information: k_{pub} and $Ex(*)$.

2.3 Error correcting issue

In the watermark embedding procedure, the image is encrypted, watermarked and decrypted in sequence. Due to the characteristics of cryptosystem, it's possible that small noise signal in the encrypted image will be expanded when the image is decrypted. This will surely interfere with the performance of the watermark system. To overcome this problem, we'll make some improvements in the proposed system.

To eliminate the negative effect of noise signal, error correcting code (ECC) is an effective resolution both in time and cost. Here, we utilize turbo code, a relative new coding technique which is often used in

communicating error correction, in the watermark system.

2.3.1 Turbo code

Turbo code is a new member of error correcting codes that came along with a practical decoding algorithm. Parallel concatenation of convolutional code is used to give the code structure so it can be decoded easily. Pseudorandom interleaving is used to give the code performance which approaches that of random coding in Shannon's theory. The original turbo code is a parallel concatenation of two recursive systematic convolutional (RSC) encoders, while the turbo decoder consists of two concatenated decoder of the component codes separated by the same interleaver. The component decoder is based on a maximum a posteriori (MAP) probability algorithm or a soft output Viterbi algorithm (SOVA) generating a weighted soft estimate of the input sequence. The iterative process performs the information exchange between two component decoders to achieve optimum coding performance.

For the reason of simplicity and length constraint, the detailed turbo coding and decoding principle won't be discussed in this paper. Readers may refer to related literature on this aspect[5].

2.3.2 Improvement to the system

We add turbo encoder and decoder in the proposed watermark system. The general procedure is shown in Fig. 3 and 4.

Compared with the system we have presented above, the difference is the presence of turbo encoder and decoder. The watermark is first turbo coded before it's embedded into the wavelet coefficients of the original image (encrypted). And also, for the image watermark, quantization should be carried out to transform the watermark to be suitable for embedding. In the process of watermark extracting, turbo decoder is added to decode the watermark signal. The other processes are the all same as those in Section 2.2, and we will not list them here to avoid duplication.

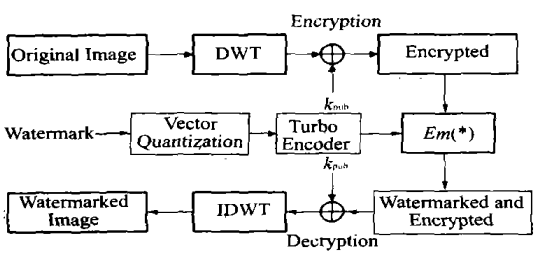

Fig 3 Improved watermark embedding plan with turbo encoder

2.4 Performance of turbo code

In order to demonstrate the effectiveness of turbo

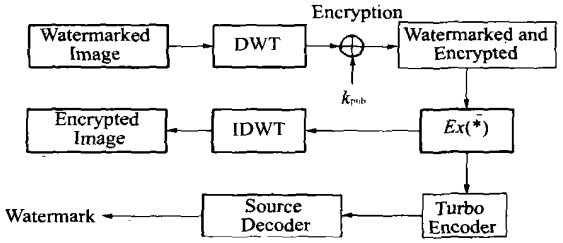

Fig 4 Improved watermark extracting plan with turbo decoder

code in the proposed system, we watermarked Lena image using turbo code. Haar wavelet transform is used, and the generated wavelet coefficients of Lena image is modified to enable the hiding of encoded data. In our test, a random message of length 1000 bits is turbo coded using two parallel convolutional encoders of rate 1/2 with the transfer function (7, 5). Punctured encoding brings about a rate of 1/2 for the turbo code while unpunctured encoding gives a rate of 1/3. The decoder uses logmap decoding with 5 iterations. Related results are shown in Fig. 5 for BER *vs.* noise addition. The difference in BER between the coded and uncoded messages is quite significant especially for lossless recovery (BER = 0). However, little difference exists between punctured and unpunctured code. And the number of bits hidden in the case of punctured code will be smaller than that of unpunctured code.

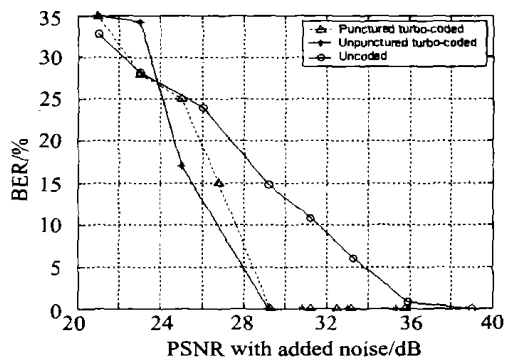

Fig 5 BER *vs.* noise for turbo coded and uncoded messages

3 Security analysis

Commonly, the possible attacks in the watermark system are as follows.

(1) To remove the watermark and get the original image: By analyzing $Em(*)$ and $Ex(*)$, attacker is able to remove the watermark information from the image. But what he gets is only an encrypted image. Without k_{pvt}, no one can decrypt the image and get the original image. So, the original version of the image is

secure in such condition.

(2) To alter the watermark: Once the attacker obtains the encrypted image, he may want to embed his fake watermark in it using $Em(\cdot)$. But he cannot get the watermarked version of the image without k_{pvt}. So the watermark in the image is protected.

(3) To destroy the watermark: To destroy the watermark means to destroy the image to some extent, and the image would become useless. The robustness of the watermark varies according to the $Em(\cdot)$, and we will do more research on this issue in the future.

4 Discussion and conclusion

This paper proposes one public watermark system using ECC. Anyone can extract and verify the watermark in the image using the public information ($Em(\cdot)$, $Ex(\cdot)$ and k_{pub}), while only those who possess kpvt can perform the watermark embedding and get the original image.

In this system, how to make the information available to the user or someone who wants to verify the watermark is a difficult thing. And how to protect or store k_{pvt} is also one big problem. Following the concept of public key infrastructure (PKI), one trusted third party should be set up to do such job, and we may call it Watermark Authority or something else similarly. This authority can manage k_{pvt} and distribute the public information related to watermark. But at present, this could only be an imagination and more work should to be done to fulfill this task.

References:

[1] BENDER W, GRUHL D, MORIMOTO N. Techniques for data hiding [J]. IBM Systems J, 1996, 35 (3): 313—336.

[2] RIVEST R L, SHAMIR A, ADLEMAN L M. A method for obtaining digital signatures and public-key cryptosystems [J]. Communications of the ACM, 1978, 21 (2): 120—126.

[3] WONG P W, MEMON N. Secret and public key image watermarking schemes for image authentication and ownership verification [J]. IEEE Transactions on Image Processing, 2001, 10 (10): 1593—1601.

[4] MALLAT S G. Multifrequency channel decompositions of images and wavelet models [J]. IEEE Transactions on Acoustics, Speech, and Signal Processing, 1989, 37 (12): 2091—2110.

[5] BERROU C, GLAVIEUX A. Near optimum error correcting coding and decoding: turbo-codes [J]. IEEE Transactions on Communications, 1996, 44 (10): 1261—1271.

采用纠错码的公开数字水印

杨　青, 陈克非

(上海交通大学计算机科学与工程系, 上海 200030)

摘　要: 提出了一种采用纠错码的可以公开检测的水印方案。水印的嵌入和提取算法都是公开的, 公钥系统取代了普通的水印密钥。任何人都可以提取并检测嵌入在图像中的数字水印, 但是却不能破坏或更改水印, 如果没有相应的私钥也无法获得原始图像。纠错码用于消除水印嵌入/提取和图像加密过程中噪声的负面影响。

关键词: 数字水印; 公钥系统; 纠错码; 离散小波变换

中图分类号: TP309