Neurocomputing 82 (2012) 62–68

Contents lists available at SciVerse ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Reversible watermarking via extreme learning machine prediction

Guorui Feng*, Zhenxing Qian, Ningjie Dai

School of Communication and Information Engineering, Shanghai University, Shanghai 200072, China,

ARTICLE INFO

Article history:
Received 6 February 2011
Received in revised form
2 September 2011
Accepted 3 October 2011
Communicated by G.-B. Huang
Available online 29 December 2011

Keywords:
Down-sample pattern
Reversible watermarking
Global regression
Extreme learning machine

ABSTRACT

In this paper, we attempt to construct a novel framework of reversible watermarking. This work is based on the difference-image histogram shift. De-correlation is the core of high capacity data-hiding in histogram-shift techniques. For the sake of higher payload, we choose the down-sample pattern as reference set. For each layer, prediction points are obtained in terms of points from the reference set. The full-resolution image quality reconstructed determines to reversible watermarking performance. When existing the prior knowledge, an effective regression method named extreme learning machine is utilized to estimate missing pixels. It can yield high-quality recovery image. Compared to other better algorithms on state of the art, the proposed method achieves higher capacity gain of watermarked images with the similar distortion.

1. Introduction

Copyright protection has become more and more serious problem because of the growing applications of digital media over the Internet. Digital watermarking is one of the valid methods for this problem. In general, the traditional watermarking makes secret data imperceptible to the attacker. Meanwhile, the distortion caused during embedding is often irreversible. In some specific occasions, for instance, high-quality witness images are very helpful for the correct judgement. Any alteration of this sort of images is prohibited. Thus, the reversible recovery of cover image plays a role part for these applications. For the sake, reversible watermarking is suggested in the digital content. It is an important branch of watermarking and is appreciated that the original media can be losslessly recovered after extracting stego-data. In this paper, we only refer to digital images. During the course extracted, we recover losslessly both watermarking information and original images. At this time, watermarking bits usually carry out the ownership protection and cover essential messages. Two key attributes of reversible watermarking are transparency and payload. Reversible watermarking desires high embedding payload and content distortion as low as possible. Two requirements conflict each other. Generally speaking, reversible information hiding cannot assume the robustness against any attack.

After reversible watermarking idea proposed in [1], to authors' knowledge, it had been attracted attentions of some scholars at the earliest era. From then on, some schemes had been proposed. According to the image format, these schemes could be simplified into compression-based and non-compression-based approaches [2]. In this paper, we only refer to the non-compression-based scheme.

The formal concept was invented at the spatial domain appeared in an authentication method in a patent [3]. Data were embedded using addition modulo 256. The key of reversible watermarking was to compress original storage space in the lossless way in order to cover the extra information. Based on this idea, Fridrich et al. compressed one of the least significant bits (LSBs) level of the quantized discrete cosine transform (DCT) coefficients to cover some bits losslessly [4]. Later, based on integer wavelet transform (IWT), reversible watermarking was also developed [5]. Because of the superior decorrelation capability of IWT, this algorithm embedded data into the middle bit-planes of the IWT coefficients to avoid the overflow and underflow case with relatively larger capacity.

In addition, the breakthrough idea of difference expansion (DE) was suggested by Tian [6]. He employed the difference and average values of close pixels to embed secret bits. The plus and minus operators calculated the original value. The roundoff was deterministic to hide information. Meanwhile, DE reversible watermarking brought higher stego-capacity. Furthermore, Alattar et al. [7] generalized Tian's method to arbitrary vectors. They employed four neighboring pixels to carry more of secret data. Another novel technique based on histogram-shift was presented by Ni et al. [8]. The histogram of pixels in the cover image was designed to embedding messages. Those pixels between the peak and zero pair were reasonable space to carry some bits. The number of pixels at the peak value position determined the maximal payload capacity for embedding

* Corresponding author.
E-mail addresses: fgr2082@yahoo.com.cn (G. Feng), zxqian@shu.edu.cn (Z. Qian), chinadai1987@sina.com.cn (N. Dai).

0925-2312/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.neucom.2011.10.028

messages. Later, regarding to evaluate blocks, watermarking embedding could adaptively discard unsuitable blocks [16]. Combining the DE with histogram-based method performed the more effectiveness in both capacity and transparency [9,10]. In [9], histogram shifting was incorporated into Tians difference expansion technique to cover the location map as side information. As well, Hu et al. [10] focused on improving the overflow location map after DE-based reversible watermarking. The efficient location map of payload-dependent overflow could increased the payload capacity. Recently, binary tree that predetermined the multiple peak points was utilized to embed watermarking [11]. This method had the better performance under the large capacity. Another advantage was to achieve large hiding capacity while preserving low distortion. To achieve a higher capacity, the residual image instead of its original version was selected to embed the watermarking information [17].

Recently, new methods effectively dealt with the tradeoff of the payload and transparency. For example, by local optimal decorrelating prediction in the local block, three prior points estimated the rest point used in [9,10,12]. Another effect strategy chose the subsampled pattern [13–15]. A low resolution version was fixed firstly. The better full-resolution image would be created via these reference points. Luo et al. [13] chose a demosaic-like scheme to estimate the difference signals by linear minimum mean square-error estimation (LMMSE) technique. It showed the better de-correlation performance. Currently, many researches pay attention to difference-image histogram-shift method. In particular, it is usually desired the high-quality image restored. To increase the payload, recent approaches [11,13] also considered the multilayer watermarking embedding.

The rest of manuscript is organized as follows. Section 2 describes the related background of a kind of down-sample decorrelated algorithm. Section 3 presents a regression method. In Section 4, we introduce extreme learning machine (ELM) regression method. It is the key of prediction in de-correlation and replies on the better neural network model. Next section, we propose reversible watermarking scheme. As a special issue, the overflow and underflow will be highlighted. The experimental results and conclusion are drawn in Sections 6 and 7, respectively.

2. Reversible watermarking prediction art

In this section, a reversible watermarking framework techniques based on histogram shift is briefly introduced. The requirement on embedding large amount of payload as many as possible, meanwhile, low embedding distortion is also desired. At the extracted phase, embedding data and original images can be obtained simultaneously.

Accordingly, the mathematical expression during the embedding phase is defined by

$$F_w = E(F, W, K), \tag{1}$$

where F_w is the watermarked image, W denotes watermarking information and K is the key. Many reversible methods ignore the security. Their security of the scheme is supported by encrypting watermarking bits instead of encrypting the embedding algorithm. At this time, the equation mentioned becomes

$$F_w = E(F, \hat{W}), \tag{2}$$

where $\hat{W} = S(F, W, K)$. The proposed method overcomes this drawback. The main body of the technique satisfies Kerckhoffs principle. The decrypting party must have access to the private key utilized to encrypt the body of this algorithm. The watermarking embedding is cooperated with key access. If malicious attacks do not know this key, they cannot obtain arbitrary corresponding information.

The inverse process deals with the extraction of useful data. The reversible watermarking need recovery F,W without distortion as shown in

$$(F, W) = D(F_w, K). \tag{3}$$

Recently efficient algorithms were most based on embedding approaches over the difference-image. A common feature of these approaches was the use of some decorrelating operator to create the higher peak of the magnitude histogram. Tian pointed that the algorithm need reversibly embedded the data in the better decorrelated components [6].

2.1. Generally de-correlate operator

In Ref. [11], authors proposed subtracting operator of the nearest pixels depicted by

$$d = |x - y|, \tag{4}$$

where d is the difference value, x,y is a neighbor pixel pair. Another better operator is used in [9,10]. It could obtain the higher peak value of the difference-image. This operator was

$$d = \begin{cases} \max(a,c) - x, & \text{if } b \le \min(a,c) \\ \min(a,c) - x, & \text{if } b \ge \max(a,c), \\ a + c - b - x, & \text{otherwise} \end{cases} \tag{5}$$

where a,b,c are in right, diagonal and lower sequence of x.

2.2. Sample prediction pattern

Consider a gray image $\mathbf{F}$ with the $M \times N$ full-resolution size, each entry F_{ij}, the subscript $i \in [1, \ldots, M]$ and $j \in [1, \ldots, N]$ with the level $[0, 255]$. Separate the image to two non-overlap regions of Ω and $\overline{\Omega}$. Now we divide the image F into two subimages of $\mathbf{F}(\Omega)$ and $\mathbf{F}(\overline{\Omega})$. In general, we assume that the main aim of the analysis is to obtain the minimization of the mean squared prediction error risk.

Define the general optimization problem:

(a) Forward processing chain

$$\hat{\mathbf{F}}_o(\overline{\Omega}) = \arg\min_{\hat{\mathbf{F}}} E\{\|\hat{\mathbf{F}}(\overline{\Omega}) - \mathbf{F}(\overline{\Omega})\| \,|\, \mathbf{F}(\Omega)\}. \tag{6}$$

After data are reversibly embedded, we update $\hat{\mathbf{F}}(\overline{\Omega})$ to $\hat{\mathbf{F}}_w(\overline{\Omega})$.

(b) Backward processing chain

$$\check{\mathbf{F}}_o(\Omega) = \arg\min_{\check{\mathbf{F}}} E\{\|\check{\mathbf{F}}(\Omega) - \mathbf{F}(\Omega)\| \,|\, \hat{\mathbf{F}}_w(\overline{\Omega})\}. \tag{7}$$

Note that $\hat{\mathbf{F}}_o(\overline{\Omega})$ and $\check{\mathbf{F}}_o(\Omega)$ are desired unbiased estimations of $\mathbf{F}(\overline{\Omega})$ and $\mathbf{F}(\Omega)$. Furthermore, $\hat{\mathbf{F}}_w(\overline{\Omega})$ denotes the watermarked image.

2.3. Bayer sample decorrelation pattern

In this subsection, we describe the related background of a kind of down-sample decorrelating algorithm. The sample pattern is similar to the well-known Bayer color filter array (CFA). Down-sample-based prediction firstly gives the low-resolution image as the reference set. The full-resolution image will be constructed by interpolation processing chain. In Ref. [13], authors suggested a type of sample pattern. These reference points could estimate rest points in multi-step estimation. In image sensor fields, the high quality of raw sensor data captured by electronics systems with a color filter array is the key in digital photography with the pocket devices. A type of CFA pattern showed the most widely used as Bayer CFA pattern [23]. It could be found that the green