Digital Signal Processing 73 (2018) 83–92

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Fast fragile watermark embedding and iterative mechanism with high self-restoration performance

Sergio Bravo-Solorio [a], Felix Calderon [b,*], Chang-Tsun Li [c], Asoke K. Nandi [d]

[a] Research & Innovation Department, DEIPI.COM S.A. de C.V., Mexico
[b] Univeridad Michoacana de San Nicolas de Hidalgo, División de Estudios de Posgrado, Facultad de Ingeniería Eléctrica, Santiago Tapia 403, Col. Centro, Morelia, Michoacan 58000, Mexico
[c] School of Computing and Mathematics, Charles Sturt University, Wagga Wagga, NSW 2650, Australia
[d] Department of Electronic and Computer Engineering, Brunel University London, London, UK

ARTICLE INFO

Article history:
Available online 20 November 2017

Keywords:
Fragile watermarking
Self-restoration
Image authentication
Erasure channel
Tornado codes

ABSTRACT

This paper presents a new algorithm to reduce significantly the computational cost of one of the best methods with self-recovery capabilities in the fragile watermarking literature. This is achieved by generating two sequences of reference bits associated to the 5 most significant bit-planes (MSBPs) of the image. The reference bits and some authentication bits are then allocated to the 3 least significant bit-planes (LSBPs) of the image. The receiver uses the authentication bits to localise altered pixel-blocks and then executes an iterative restoration mechanism to calculate the original value of the watermarked pixels. Experimental results demonstrate that the embedding method executes significantly faster compared to the state-of-the-art method while achieving a high restoration performance.

1. Introduction

The proliferation of powerful image editing software has raised serious concerns about the reliability of digital images, specially in application fields where altered content may lead to unacceptable consequences, e.g. law enforcement applications.

Fragile watermarking technology is aimed at exposing changes in the image content by identifying alterations on information embedded *a priori* (i.e., *watermark*). The fact that the embedded watermark undergoes the same distortions as the *host* image opens up the possibility of providing additional capabilities, such as *tampering localisation* and *self-recovery*.

Tampering localisation refers to the ability of identifying distorted regions, while verifying the integrity of the remainder of the image [1–4]. Self-recovery, on the other hand, refers to the ability of restoring the image content to its original state prior to the manipulation. The restoration can be either *approximate* or *exact*. Schemes with approximate restoration capabilities aim to recover a coarse version of the original content. For example, Qin et al. [5] embed reference bits generated from bits of vector quantisation (VQ) indices, along with some authentication bits, in the 3 LSBPs of the image. In the receiver side, manipulated pixels are located and the reference bits retrieved from unaltered pixels are used to recover a close approximation of the original content. This method is capable of restoring altered regions that extend up to 60% of the image. In [6], Qin et al. generate some reference bits from the mean value calculated from overlapping blocks of pixels, which are embedded into 1 or 2 LSBPs of the image. At the receiver end, manipulated regions are located and the mean values are reconstructed. A recovery operation is then conducted for every tampered pixel depending on its location in the overlapping blocks. The embedding strategy produce less embedding distortion and yet is capable of restoring images with manipulated regions of up to 45% of the image. Although these schemes can reconstruct considerably large tampered regions [7–18], the quality of the restored content may be insufficient for some applications.

Methods with exact restoration capabilities can recover the original content perfectly, provided that the altered area is not too extensive. In [19,20] Reed–Solomon error correction codes are used to calculate parity bits for every row and column of the cover image. The encrypted parity bits are embedded in the 2 LSBPs of the image. This scheme is capable of recovering up to 13 pixels in a single row or column and localising the distortions even if restoration is no possible. In Zhang and Wang's scheme [21], some reference bits are generated with the 5 MSBPs of the image. The receiver localises the altered regions by identifying changes in some authentication bits and then estimates the original pixels by means of exhaustive attempts. Nonetheless, the number of restored

* Corresponding author.
E-mail addresses: bravo.solorio@deipi.com (S. Bravo-Solorio), calderon@umich.mx (F. Calderon), chli@csu.edu.au (C.-T. Li), asoke.nandi@brunel.ac.uk (A.K. Nandi).

https://doi.org/10.1016/j.dsp.2017.11.005

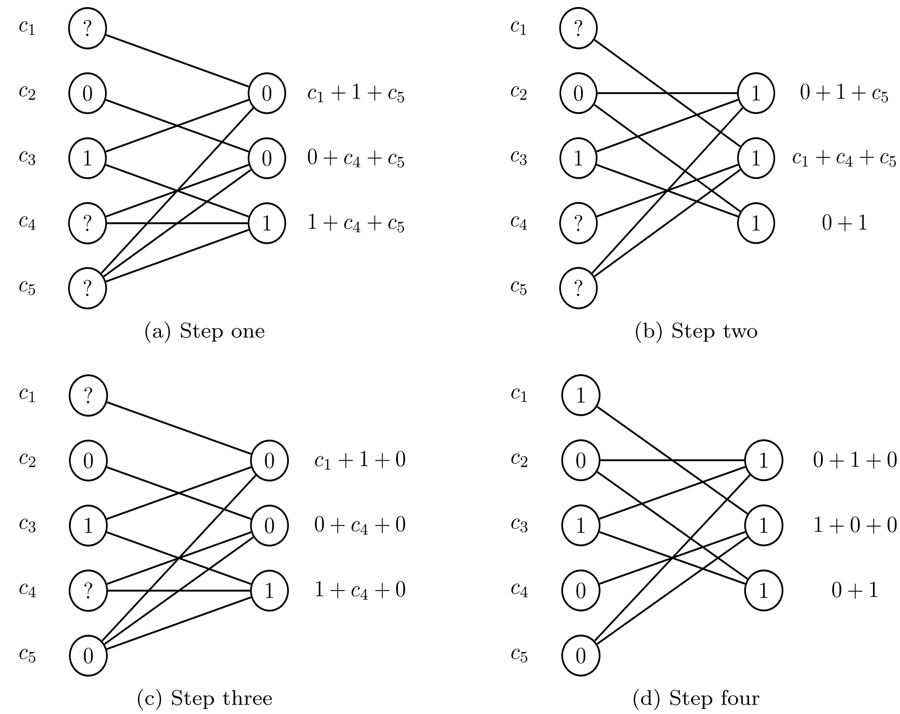

Fig. 1. Bipartite graphs used for decoding algorithm.

pixels drops sharply for tampered areas that cover above 6.6% of the image. To provide a more gradual decline of the restoration performance, an iterative approach was introduced in [22]. In [23], the reference bits and some authentication bits are reversibly embedded. At the receiver side, the surviving reference bits and the unaltered pixel bits are employed to estimate the original value of the altered pixels by means of solving some binary linear equation systems. With this method, up to 3.2% of the image can be restored. Furthermore, when the reference bits and the authentication bis are embedded with a non-reversible mechanism, up to 24%–28% of the image can be restored, depending on the initial settings and the image size [24]. However, the computational cost of the embedding algorithm may render the scheme unsuitable for real scenarios, wherein the watermark must be embedded at the time of capture [25,26].

In this paper, the problem of the embedding time consumed by the method proposed by Zhang et al. [24] is addressed. Inspired by the iterative approach of Tornado codes [27], two sequences of independent reference bits are generated as a result of associating every bit in the 5 MSBPs of the image to two different subsets. The restoration method executes an iterative mechanism to recover the altered pixels. The proposed method is detailed in Section 2. In Section 3, the restoration performance and the computational cost of the proposed approach are analysed, and some experimental and comparison results are reported in Section 4. Finally, some conclusions are given in Section 5.

2. Proposed watermark insertion method

The proposed iterative restoration approach is inspired by a class of erasure codes known as Tornado codes [27]. Typical Tornado codes are comprised of a series of random irregular bipartitie graphs. For a bipartitie graph, the left-most L nodes represent information bits which are to be transmitted reliably across the erasure channel. The nodes in all subsequent stages represent parity check bits, which form a sequence of graphs $(G_0, G_1, \cdots G_m, D)$. Assume that each stage G_i has $L\beta^i$ input bits and $L\beta^{i+1}$ output bits, for all $0 \leq i < m$ and $0 < \beta^i < 1$. Thus, the number of nodes shrinks by a factor β^i at the i-th stage except for the last one.

Unlike Tornado codes, which rely on a series of G_i bipartitie graphs to calculate the parity bits, in our approach we use a pair of graphs G_o and G_e. In the mathematical field of graph theory, a bipartite graph (or bigraph) is a graph whose vertices can be divided into two disjoint sets U and V, such that every edge connects a vertex in U to another in V. Both bigraphs will receive L information bits in parallel and calculate βL parity bits with a shrinking factor β. The L information bits and the $2\beta L$ parity bits are sent through the erasure channel.

To illustrate the rationale behind the proposed iterative restoration mechanism, consider the two example matrices $\mathbf{A}_o$ and $\mathbf{A}_e$ defined in (1).

$$\mathbf{A}_o = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad \mathbf{A}_e = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix} \tag{1}$$

The bigraphs formed by the matrices above are shown in Fig. 1a and Fig. 1b, respectively. In the embedding process, two vectors, $\mathbf{r}_o = \mathbf{A}_o\mathbf{c}$ and $\mathbf{r}_e = \mathbf{A}_e\mathbf{c}$, are calculated using arithmetic modulo 2.

To retrieve the information, we use a process similar to the Tornado codes but alternating the solutions between the pair of graphs G_o and G_e. For example, Fig. 1 illustrates the steps followed to recover the missing information bits c_1, c_4 and c_5. Although, in the first step, it is impossible to calculate the missing values, the value of the bit c_5 can be calculated in the second step. In third step, it is possible to calculate the bits c_1 and c_4, given the bits c_2, c_3 and c_5. Finally, in the fourth step, it is verified that all the missing bits have been fully calculated and the iterative process ends.

2.1. The protected and discarded bit-planes

Given a 256 grey-scale image, sized $N_r \times N_c$ and let $p_n \in [0, 255]$ be a pixel, for $n = 1, \ldots, N$ $(N = N_r \times N_c)$. Every pixel p_n