Signal Processing: *Image Communication* 25 (2010) 10–17

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

Secure reversible visible image watermarking with authentication

Han-Min Tsai [a], Long-Wen Chang [a,b,*]

[a] *Department of Computer Science, National Tsing Hua University, No. 101 Kuang Fu Road, Hsinchu 300, Taiwan*
[b] *Institute of Information Systems and Applications, National Tsing Hua University, Hsinchu, Taiwan*

ARTICLE INFO

Article history:
Received 5 December 2008
Received in revised form
10 November 2009
Accepted 18 November 2009

Keywords:
Visible watermarking
Reversible data embedding
Image authentication
Lagrange multipliers

ABSTRACT

This paper proposes a secure reversible visible watermarking approach. The proposed pixel mapping function superposes a binary watermark image on a host image to create an intermediate visible watermarked image. Meanwhile, an almost inverse function generates the recovery data for restoring the original pixels. To prevent unauthorized users from approximating the original pixels in the watermarked region, this method adds an integer sequence in the intermediate watermarked image. The sequence is composed of integers generated by two random variables having normal distributions with zero means and distinct variances. The variances facilitate a trade-off between the watermark transparency and the noise generated by unauthorized users. The proposed method also uses Lagrange multipliers to find the optimized variances for the trade-off. Finally, this method uses reversible data embedding to embed the recovery data and hash value for reversibility and authentication, respectively. Experimental results show the watermark visibility for test images along with the watermark transparency for different variances. Using the optimized variances, the watermarked image is at the balance between the watermark transparency and the unauthorized-user-generating noise.

1. Introduction

Advances in digital technology allow people to easily create valuable digital images and share them on Internet. At the same time, however, the digital images are easily duplicated and used illegally. Laying an identity logo (watermark) on an original image helps deter its unauthorized use. The process of superposing a visible watermark on a host image is called visible watermarking, and the superposed image is the visible watermarked (VW) image. The three major requirements for VW images are visibility, transparency, and robustness [1]. In other words, (1) the logo must be clearly visible on the watermarked image, (2) the edges of the host image beneath the logo must not be too distorted for transparency, and (3) the watermark should not be easily removed for robustness. However, one requirement is usually the trade-off of another one. For example, a very translucent visible watermark implies that the approximation of the original pixels is easy. That is, the watermark logo is almost removed, which contradicts the robustness. Hence, users should decide the priority order for the three requirements in their own uses.

Conventional visible watermarking, e.g., [2,3], usually produces a translucent watermarked image by a weighting addition $i' = \alpha i + (1-\alpha)w$, where i, w, α, and i' denote the host signal, the watermark signal, weighting factor, and the superposed signal, respectively. Using the weighting addition preserves the edges beneath the watermark very well. However, the real number i' must be truncated to a round number for digital images. Lossless recovery of the original image becomes difficult if the truncated decimal requires a large bit rate. If the original image can be

* Corresponding author at: Department of Computer Science, National Tsing Hua University Hsinchu, No. 101 Kuang Fu Road, Hsinchu 300, Taiwan.
E-mail address: lchang@cs.nthu.edu.tw (L.-W. Chang).

0923-5965/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.image.2009.11.002

perfectly restored from the visible watermarked image, the following models may be attractive. Mintzer et al. [4] proposed a reversible visible watermark model in which the watermarked image can be viewed for free and the original image can be restored upon paying an additional fee. Yongjian and Byeungwoo [5] treated a visible watermark as a tag or ownership identifier that must be completely removable. This model is useful for medical or military images, which have zero tolerance for even small distortions caused by watermarking. In addition, a visible watermark can serves as a tag to protect patient privacy for medical images, or to prevent information disclosure for military images.

A removable visible watermarking scheme [6] creates a pre-watermarking template based on a user key, and then applies conventional visible watermarking with a human visual model (HVS) on the template to generate a visible watermarked image. Similarly, lossless recovery is difficult when the truncated decimal needs a large bit rate. A user-key-dependent template enables authorized users to restore images with high quality, whereas unauthorized users can only restore images with low quality. Shu-Kei et al. [7] proposed a lossless visible watermarking using two bijective algorithms: *the pixel value mapping algorithm* (PVMA) and *the pixel position shift algorithm* (PPSA). In their method, pixels are first processed by the PVMA, and then the PPSA forms visible watermarked pixels. Distortion-free recovery is easily performed by applying the inverse PPSA followed by the inverse PVMA on the watermarked pixels. They also proposed adding random numbers on the watermarked pixels for security. The current paper extends this approach for watermark transparency adjustments. Yongjian and Byeungwoo [5] also proposed a reversible visible watermarking scheme. It contains two phases: *showing the visible watermark* and *embedding the recovery data*. Hu et al. showed a visible watermark by replacing the most significant bit (MSB) plane in the watermark region of the original image. The original MSB is then embedded in the region except the watermarked region.

This paper proposes a non-bijective pixel value mapping function to create a visible and moderately translucent watermark on the host image. The residual data caused by the mapping is recorded as the recovery data. The proposed method also adds a sequence of random integers on the watermarked region. This added sequence not only protects the watermarked pixels, but also facilitates the trade-off between transparency and robustness. Finally, an existing reversible data embedding method embeds the recovery data and the hash value of the original image in the watermarked image.

2. Proposed secure reversible visible watermarking

The proposed secure reversible visible watermarking (SRVW) in Fig. 1 contains three stages: (1) visible watermarking, (2) protection and transparency adjustment, and (3) reversible data embedding. Stage 1 superposes the watermark and the host image by the proposed pixel value mapping technique. Meanwhile, the information loss caused by this mapping is recorded as recovery data for restoring the original image. To authenticate the recovered image, authentication data are recorded as well. In this study, the hash value of the original image is encrypted by the secret key K_1 as the authentication data. Stage 2 adds a key-generated integer sequence in the visible watermarked region to prevent restoring an almost-original image. This added sequence also controls the trade-off between transparency and robustness. Researchers have recently proposed a variety of reversible data embedding algorithms, e.g., [8–16]. Stage 3 embeds the recovery data and the authentication data using an existing reversible data embedding algorithm [10]. The following describes some notations used in the proposed method. Note that the pixel values of the original images and watermark image are all integers.

I: An 8-bit grayscale host image. $I \in M^{m \times m}$, $0 \le I(x,y) \le 255$.

W: A 1-bit watermark image. $W \in M^{n \times n}$, $0 \le W(x,y) \le 1$, $n \le m$.

R: A square subimage in the host image to show the watermark. $R \in M^{n \times n}$, $0 \le R(x,y) \le 255$.

R_W: The superposed image of R and W. $R_W \in M^{n \times n}$, $0 \le R(x,y) \le 255$.

2.1. Visible watermarking

To show the watermark on a host image, first superpose the two images R and W by the pixel value

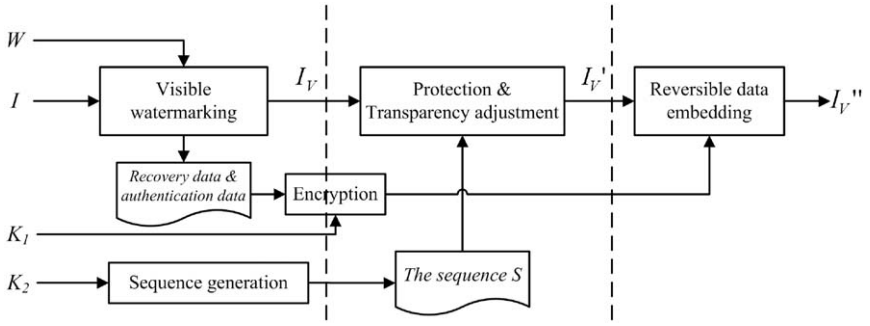

Fig. 1. The proposed secure reversible visible watermarking (SRVW).