

Correspondence

Comments on “An SVD-Based Watermarking Scheme for Protecting Rightful Ownership”

Xiao-Ping Zhang, *Senior Member, IEEE*, and Kan Li

Abstract—In a recent paper by Tan and Liu [1], a watermarking algorithm for digital images based on singular value decomposition (SVD) is proposed. This comment demonstrates that this watermarking algorithm is fundamentally flawed in that the extracted watermark is not the embedded watermark but determined by the reference watermark. The reference watermark generates the pair of SVD matrices employed in the watermark detector. In the watermark detection stage, the fact that the employed SVD matrices depend on the reference watermark biases the false positive detection rate such that it has a probability of one. Hence, any reference watermark that is being searched for in an arbitrary image can be found. Both theoretical analysis and experimental results are given to support our conclusion.

I. INTRODUCTION

In the above paper [1], the authors proposed a new image watermarking scheme by embedding watermark into the singular value decomposition (SVD) domain. First the SVD is performed on the original $M \times N$ image A (see [1, eq. (5)]), i.e.,

$$A \Rightarrow USV^H \quad (1)$$

where U and V are an $M \times M$ orthogonal matrix and $N \times N$ orthogonal matrix, respectively, and S is an $M \times N$ diagonal singular value matrix. A spread spectrum watermark matrix W is then added into the matrix S , and SVD is performed on the new matrix $S + \alpha W$ to get U_w, S_w , and V_w , where α is the scaling parameter that determines the strength of the watermark W

$$S + \alpha W \Rightarrow U_w S_w V_w^H. \quad (2)$$

Then the watermarked image A_w is obtained by

$$U S_w V^H \Rightarrow A_w. \quad (3)$$

In watermark extraction, a possibly distorted watermark W^* is extracted from the possibly distorted watermarked image A_w^* by essentially reversing the above watermark embedding steps. The watermark extraction and detection can be described as follows (see [1, eq. (6)]):

$$A_w^* \Rightarrow U^* S_w^* V^{*H} \quad (4)$$

$$U_w S_w^* V_w^H \Rightarrow D^* \quad (5)$$

$$(D^* - S)/\alpha \Rightarrow W^*. \quad (6)$$

Note that matrices U_w, S, V_w are required in watermark extraction. Like other spread-spectrum technique-based schemes, the similarity of W^* and W is measured to identify the extracted watermark W^* [2].

Manuscript received March 11, 2003; revised October 29, 2003. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Fernando M. B. Pereira.

The authors are with the Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON M5B 2K3, Canada (e-mail: xzhang@ee.ryerson.ca).

Digital Object Identifier 10.1109/TMM.2005.843357

We argue that the above watermarking method is fundamentally flawed. Please note that in (2), since S is just a diagonal matrix, the matrices U_w and V_w represent the subspace of a slightly modified watermark W , which only differs from the original watermark in diagonal values. As known, the SVD subspace can preserve the major information of an image [as it is used in (3)]. Therefore, in detection step (5), no matter what value the diagonal matrix S^* takes, the resulting matrix D^* is in the same SVD subspace defined by the diagonally modified watermark W . In other words, (5) effectively “stamps” the information of watermark W on D^* no matter what A_w^* and the real W are. Note that (6) changes only the diagonal values of D^* . Hence, the “extracted” watermark W^* will have high correlation with the watermark W whatever A_w^* is.

II. EXAMPLES

In the following example, a 256×256 image “Lena” is used as the host image A . Image “Panda” is used as watermark W_p and image “Monkey” is used as watermark W_m . The two watermarks are applied to the host image, respectively, to generate two watermarked images A_{wp} and A_{wm} according to (1)–(3) and to obtain the matrix S and SVD signature matrices U_{wp} and V_{wp} for the watermark W_p . The scaling parameter $\alpha = 1/255$ in this experiment. At the detector end, we do not know whether there is a watermark embedded or which watermark is embedded. Now we try to detect whether watermark W_p (“Panda”) is embedded in the watermarked image A_{wm} (with watermark W_m —“Monkey”) according to (4)–(6), as follows:

$$A_{wm} \Rightarrow U_{wm}^* S_{wm}^* V_{wm}^{*H} \quad (7)$$

$$U_{wp} S_{wm}^* V_{wp}^H \Rightarrow D_{mp} \quad (8)$$

$$(D_{mp} - S)/\alpha \Rightarrow W_{mp}. \quad (9)$$

Ideally, the extracted watermark W_{mp} should have no correlation with “Panda” since the embedded watermark is a “Monkey.” However, as we predicted in Section I, the extracted watermark W_{mp} is a “Panda” instead of the real embedded watermark “Monkey,” though there are slight differences in diagonal values, as shown in Fig. 1. The correlation coefficient of the extracted watermark with the reference watermark “Panda” is 0.9982. That is to say, we detected a “Panda” from a watermarked image with a “Monkey” watermark using the watermarking method in [1]. The fundamental flaw is that the reference watermark “Panda” is “stamped” anyway at the detector end by (5), i.e., (8).

Note that the experiments in [1] are also flawed. Unlike the example we presented here, the embedded true watermark and the reference watermark that generates the SVD matrices employed in the detector are the same in [1]. The correlations of the extracted watermark with a set of watermarks are then calculated. In such cases, the “stamped” reference watermark will certainly prevail at the detector end as we analyzed.

In short, the problem in [1] has to do with the fact that their detection stage makes use of information that is dependent on the watermark. The watermark-dependent information is so improperly used in [1] such that it does not guarantee an objective detection outcome and creates a false positive detection rate of one in the above example. We also note that such type of problems has been independently addressed in a slightly different way in a recent paper [3].

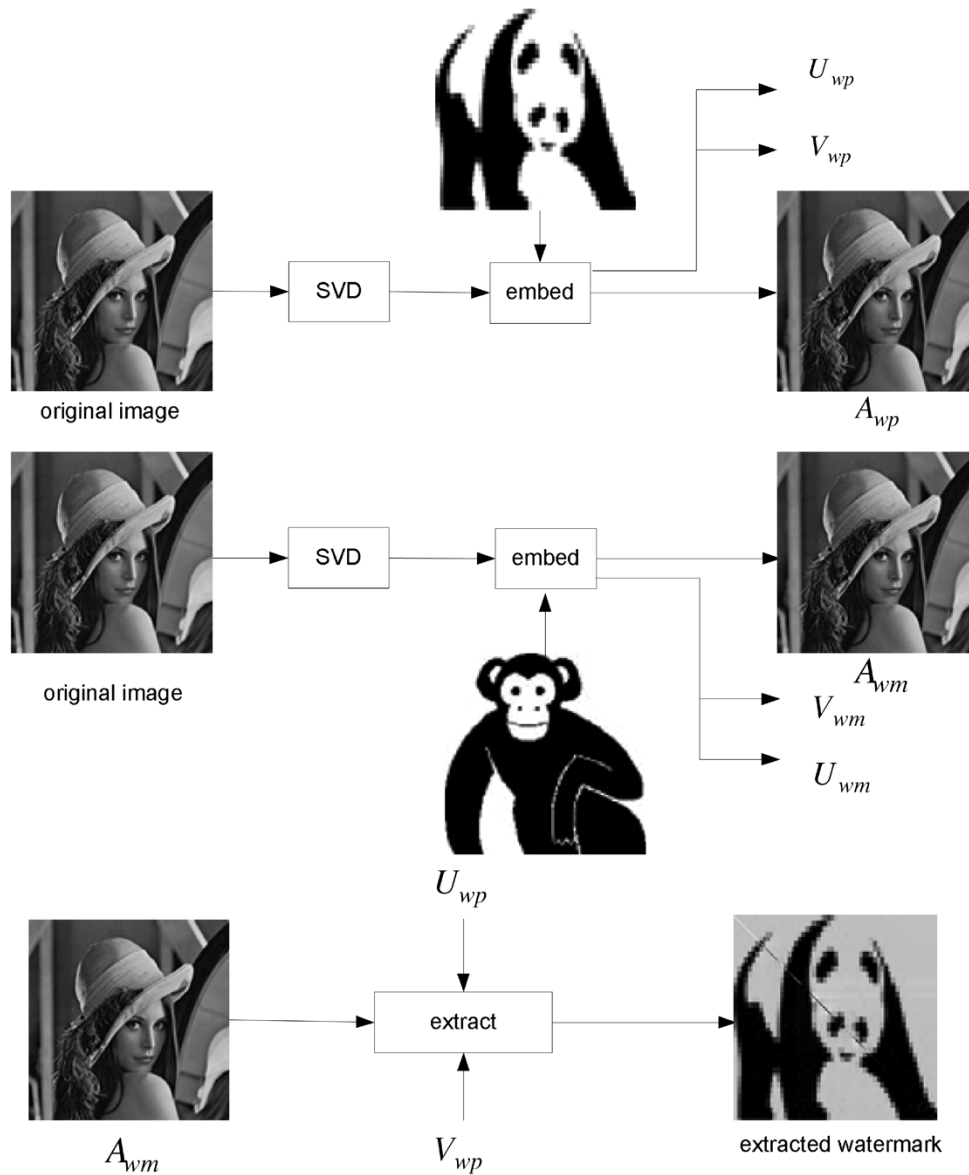


Fig. 1. Extracted watermark is determined by the pair of SVD matrices employed in the watermark detection.

REFERENCES

- [1] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia.*, vol. 4, no. 1, pp. 121–128, Mar. 2002.
- [2] I. J. Cox, J. Kilian, T. Leighton, and T. Shanon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 7, pp. 1673–1687, Dec. 1997.
- [3] D. Kundur and D. Hatzinakos, "Toward robust logo watermarking using multiresolution image fusion," *IEEE Trans. Multimedia.*, no. 1, pp. 185–198, Feb 2004, to be published.