Steganography of digital watermark based on Speed-up generalized morphological component analysis

Shaochun Ma[1,a], *Qingsheng Kong[2,b]

[1]Department of Electrical Engineering, school of Information Science and Technology, Fudan University, Shanghai, 200433, China

[2]Department of Electrical Engineering, school of Information Science and Technology, Fudan University, Shanghai, 200433, China

[a]email:mablemsc@163.com, [b]email:qskong@fudan.edu.cn

Keywords: Steganography; Digital Watermark; Arnold Scrambling; Blind Sourse Separation; Speed-up Generalized Morphological Component Analysis

Abstract. In this Letter, a novel steganography of digital watermark scheme which contains digital watermark embedding and extraction processes is proposed. The proposed scheme is based on an iterative process of Arnold scrambling transform which is controlled by secret key shared by copyright owner and authorized users, and the extension of morphological component analysis theory which utilizes morphological diversity as the kernel role in blind source separation. Images acquired in steganography experiments prove the effectiveness of proposed scheme. Both visual effect and quantitative experiment results of the Peak Signal to Noise Ratio (PSNR) index and Structural Similarity (SSIM) index confirm its steganography capability as well as its robustness to different noise attacks through communication channel.

Introduction

With the explosive growth of digital image techniques, how to efficiently protect the copyright of original image and prosecute copyright violators cause increasing concerns. As an efficacious authentication method, digital watermark has attracted great attention in the field of information security. As copyright markings, digital watermarks (DW) may be certain visual patterns (e.g., national emblem, company logo or personal sign) overlaid on original digital images [1]. Steganography is an information hiding tool to conceal the existence of important message in other information. Steganography of digital watermark can enhance the communication security since the existence of embedded digital watermark is unknown to a potential attacker.

In this Letter, we propose a novel steganography scheme of digital watermark based on Arnold scrambling transform[2] and the extension of the Speed-up generalized morphological component analysis (SGMCA) theory [3][4]. As a powerful signal processing tool, morphological diversity plays the essential role in the success of MCA [5][6]. By extending SGMCA to blind source separation (BSS) framework, the proposed scheme has a good performance on digital watermark extraction, and is robust to several noise attacks.

Proposed scheme

There are two main processes in this proposed scheme, i.e., digital watermark embedding process and digital watermark extraction process. The block diagram of whole proposed scheme is illustrated in Fig. 1.

In digital watermark embedding process, firstly a $N \times N$ image OCM contains original copyright marking is changed to digital watermark ODW for embedding through Arnold scrambling transform as follows:

$$\text{for } i = 1, \cdots, K, \ \begin{pmatrix} \acute{x} \\ \acute{y} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N), \tag{1}$$

where $x, y \in \{0,1,2, \cdots, N-1\}$ represent the positions of pixels before Arnold scrambling

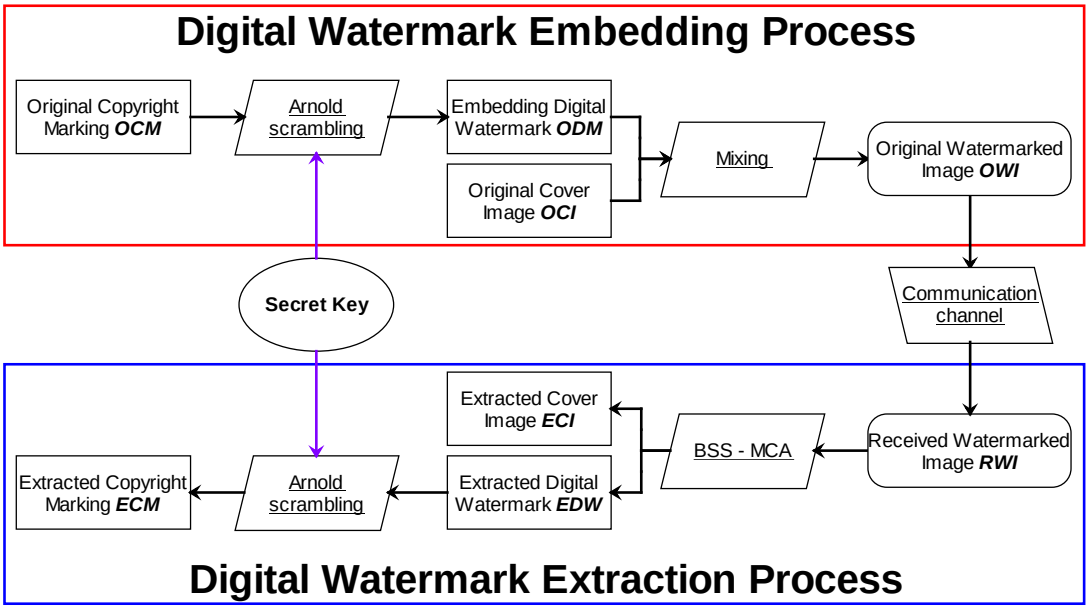


Fig. 1. Block diagram of proposed scheme

transform, while $\acute{x}, \acute{y} \in \{0,1,2,\cdots,N-1\}$ represent the positions of pixels after Arnold scrambling transform. The iteration number K is chosen as the Secret Key which is only shared by copyright owner and authorized users. After mixing digital watermark ODW with original cover image OCI, the original watermarked image OWI is obtained as follows:

$$OWI = A_1 OCI + A_2 ODW = AS, \quad (2)$$

where S is the original source matrix, and A is the mixing matrix which defines the specific contribution of original cover image OCI and embedding digital watermark ODW to original watermarked image OWI. By passing original watermarked image OWI through the communication channel, authorized users observe the received watermarked image RWI. Since there are potential noises or attacks in communication channel, so received watermarked image RWI may not be totally equal to original watermarked image OWI.

$$RWI = AS + E, \quad (3)$$

This observation model is consistent with the linear mixture model in BSS problem. The model is assumed to contain N_c channels of observation $(rwi_1, \cdots, rwi_{N_c})$, where each channel of observation $\{rwi_i\}_{i=1,\cdots,N_c}$ is a one-dimensional vector of length $M = N \times N$ by reordering all pixels in a two-dimensional observed watermarked image into it. Each observed channel is also the linear mixture of N_s vectors $(\boldsymbol{s}_1, \cdots, \boldsymbol{s}_{N_s})$ which are original sources with the same length M. Then $RWI = [rwi_1^T, \cdots, rwi_{N_c}^T]^T$ is the $N_c \times M$ observation matrix. $A = [a_1^T, \cdots, a_{N_c}^T]^T$ is the $N_c \times N_s$ mixing matrix which defines the specific contribution of each original source to each observation channel. $S = [s_1^T, \cdots, s_{N_s}^T]^T$ is the $N_s \times M$ original source matrix. $E = [\boldsymbol{\varepsilon}_1^T, \cdots, \boldsymbol{\varepsilon}_{N_c}^T]^T$ is the $N_c \times M$ matrix which is included to account for noises, attacks, as well as imperfections of linear mixture model. The proposed scheme discusses the over-determined situation where $N_c \geq N_s$, thus A has full column rank.

For example, we acquire a RGB image with the dimension of 1024×1024 in the steganography application. This image contains three color layers (e.g., Red layer, Green layer and Blue layer), and it is the superposition of two unrelated source signals. Then observation matrix RWI represents the observation of this multi-layer image. The symbol $N_c = 3$ and rwi_1, rwi_2, rwi_3 represent the Red, Green and Blue observation channels, respectively. Each observation channel contains $M = 1024 \times 1024$ pixels and each channel is the linear mixture of $N_s = 2$ original sources.

As the observation result is consist of N_c different mixtures, the source separation technique aims at restoring the original sources $\{s_i\}_{i=1,\cdots,N_s}$ by taking advantage of some information contained in the way the signals are mixed in the observation channels. In the BSS problem, both

the mixing matrix A and the original source matrix S are unknown, and they must be estimated jointly. Generally, without further a *priori* knowledge, decomposing a rectangular observation matrix RWI into a linear combination of N_s rank-one matrices is clearly an ill-posed mathematical problem. The goal of BSS problem is to utilize the additional prior constraints and to devise separation methods which can handle the contrast and diversity to disentangle the original sources.

In digital watermark extraction process, how to divide received watermarked image RWI into cover image and digital watermark is the core of the scheme. The basic concept of MCA theory is taking advantages of morphological diversity [3] as the source of discernibility among mixed signals. The proposed scheme utilizes SGMCA theory by extending its concept to BSS framework, and devises separation method which can handle the contrast and diversity to disentangle the original sources.

Our scheme supposes that the original sources $\{s_i\}_{i=1,\cdots,N_s}$ can be sparsely represent by the dictionary $D = [\Phi_1^T, \cdots, \Phi_P^T]^T$ which is the combination of P bases: $\{\Phi_i\}_{i=1,\cdots,P}$. Then each original source is the linear combination of P morphological components, while each component can be sparsely represented by a certain basis, i.e.:

$$s_i = \sum_{k=1}^{P} \varphi_{ik} = \sum_{k=1}^{P} \alpha_{ik}\Phi_k, \ \forall i \in \{1, \cdots, N_s\} \quad (4)$$

Through the estimation of A, the scheme is to seek the sparsest representation of original sources S in the dictionary D, which can be expressed by a tractable optimization problem as follows:

$$\{\tilde{A}, \tilde{S}\} = \arg\ \min_{A,S} \sum_{i=1}^{n} \sum_{k=1}^{P} \|\varphi_{ik}\Phi_k^T\|_1 + \kappa\|X - AS\|_2^2, \quad (5)$$

where the symbols $\tilde{A}, \tilde{S}$ represent the estimations of A, S. By introducing the sparse decomposition operator $\Delta_D(\cdot)$, then the unique ℓ_1 pseudo-norm sparse decomposition of RWI and S can be defined as $\Theta_{RWI} = \left[\Delta_D(rwi_1)^T, \cdots, \Delta_D\left(rwi_{N_c}\right)^T\right]^T$ and $\Theta_S = \left[\Delta_D(s_1)^T, \cdots, \Delta_D\left(s_{N_s}\right)^T\right]^T$. Therefore we can iteratively and alternately estimate both A and Θ_S in the sparse domain by solving the optimization problem as follows:

$$\{\tilde{A}, \tilde{\Theta}_S\} = \arg\ \min_{A,\Theta_S} \kappa\|\Theta_{RWI} - A\Theta_S\|_2^2 + \|\Theta_S\|_1 \quad (6)$$

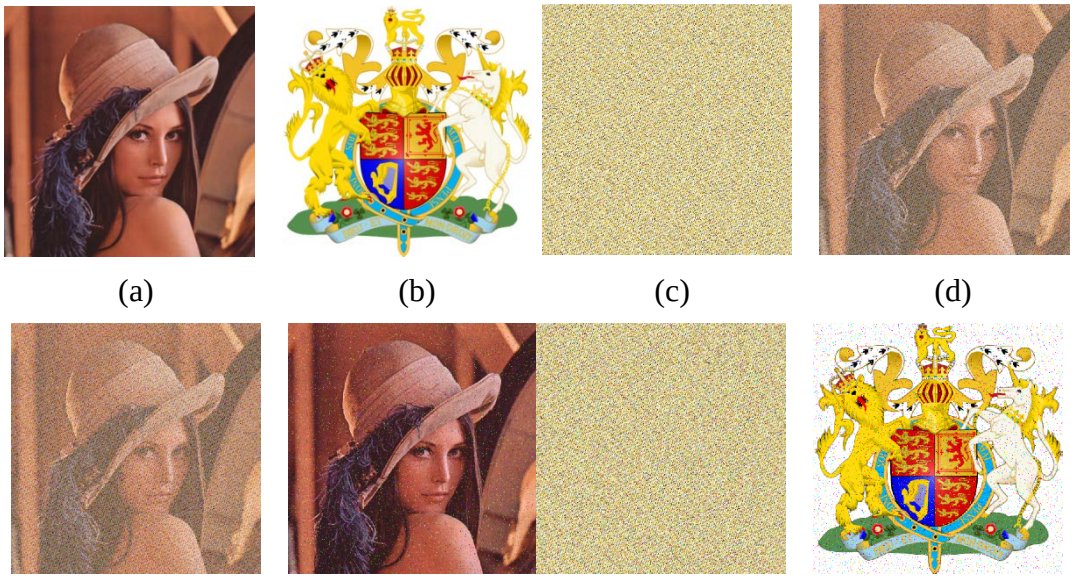
Detailed steps of BSS-SGMCA scheme:

1. Perform MCA to observations to calculate
$$\Theta_{RWI} = [\Delta_D(rwi_i)^T]^T \quad (7)$$
2. Initialize iterative number $I_{iteration}$ and inceptive threshold: $\delta^{(0)}$.
3. While No. h iterative threshold $\delta^{(h)}$ is larger than stop threshold δ_{min} which depends on the noise variance, iterative process continues.
   3.1. Assuming A is fixed, then estimate the coefficients of Θ_S.
   $$\Theta_S^{(h+1)} = \lambda_{\delta^{(h)}}\left(A^{\dagger(h)}\Theta_{RWI}\right), \quad (8)$$
   where $A^\dagger$ is the pseudo-inverse of A and λ_δ is a thresholding operator with threshold δ.
   3.2. Assuming Θ_S is fixed, then update mixing matrix A by a least-squares estimation as follows:
   $$\tilde{A}^{(h+1)} = \Theta_{RWI}\tilde{\Theta}_S^{(h)^T}\left(\tilde{\Theta}_S^{(h)}\tilde{\Theta}_S^{(h)^T}\right)^{-1} \quad (9)$$
   3.3. Decrease the threshold $\delta^{(h)}$.
4. If $\delta^{(h)} = \delta_{min}$, then stop the iterative process.
5. Reconstruct the source image S by sparse composition of $\tilde{A}^\dagger\Theta_{RWI}$ in dictionary D to get extracted cover image ECI and extracted digital watermark EDW.

Since Arnold scrambling transform is a period transform, extracted digital watermark EDW is changed to the extracted copyright marking ECM through Arnold scrambling transform with $T - K$ iterations, where the constant T is the period of Arnold scrambling transform which is depended on the size of the transformed image.

Experimental results

Experiments reported in this short communication are performed on MATLAB R2014b platform which runs in the laptop with Intel Core i5-5200U (2.20GHz). Fig. 2(a) shows the RGB Lena image with the size of 512×512 pixels which is chosen as original cover image OCI. Fig. 2(b) shows the RGB British national emblem with the size of 512×512 pixels which is chosen as original copyright marking OCM. Fig. 2(c) shows the RGB embedding digital watermark ODW with security key $K = 100$. Fig. 2(d) shows the RGB original watermarked image OWI. Fig. 2(e) shows the RGB received watermarked image RWI through the communication channel. There are salt and pepper noise attack in the communication channel. The noise density is 0.04 which affects approximately 4% of all pixels of original images. Fig. 2(f) shows the RGB extracted cover image ECI. Fig. 2(g) shows the RGB extracted digital watermark EDW. Since the dimension of the copyright marking is 512×512 pixels, the determined period T of Arnold scrambling transform is 384. So the secret key $T - K$ used to acquire extracted copyright marking ECM from extracted digital watermark EDW through Arnold scrambling transform is 284. Fig. 2(h) shows the RGB extracted copyright marking ECM.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 2. Images acquired in steganography scheme of digital watermark

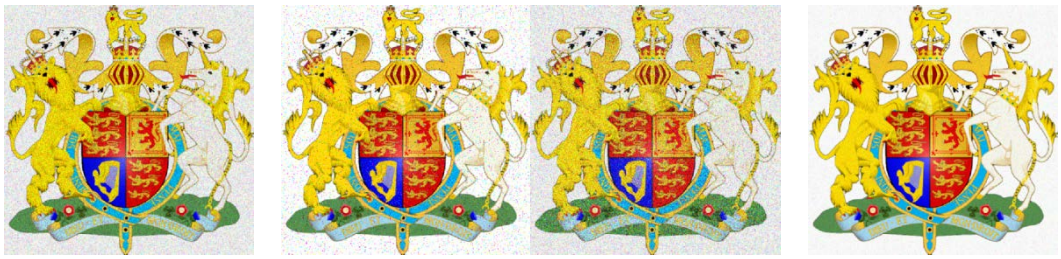
In order to make quantitative analysis, the Peak Signal to Noise Ratio (PSNR) index is calculated to assess the effect from the gray-level fidelity aspect. The Structural Similarity (SSIM) index [7] which is an image quality assessment index based on the human vision system is calculated to assess the effect from the structure-level fidelity aspect. The quantitative experiment results of original cover image OCI versus extracted cover image ECI and original copyright marking OCM versus extracted copyright marking ECM are shown in Table 1.

Table 1: PSNR (Unit: dB) and SSIM results of OCI versus ECI and OCM versus ECM

	Red Channel		Green Channel		Blue Channel		Average	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
OCI vs *ECI*	19.33	0.54	19.46	0.52	18.95	0.51	19.25	0.52
OCM vs *ECM*	17.65	0.61	17.89	0.61	17.57	0.62	17.70	0.61

To test the performance of proposed scheme and its robustness to noise attack, four kinds of noises is adopted in communication channel respectively. Fig. 3(a) illustrates the extracted copyright marking ECM after adding multiplicative noise with variance 0.04. Fig. 3(b) illustrates the extracted copyright marking ECM after adding salt and pepper noise. The noise density is 0.05 which affects approximately 5% of all pixels. Fig. 3(c) illustrates the extracted copyright marking

ECM after adding Gaussian white noise. The noise is zero mean with variance 0.05. Fig. 3(d) illustrates the extracted copyright marking ECM after adding Poisson noise. The quantitative experiment results of original copyright markings versus corresponding extracted copyright markings are listed in Table 2.



(a) (b) (c) (d)

Fig. 3. Extracted copyright markings after noise attacks

Table 2: PSNR (Unit: dB) and SSIM results of original copyright markings versus corresponding extracted copyright markings

Noise Patten	Red Channel		Green Channel		Blue Channel		Average	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Multiplicative	17.45	0.46	17.52	0.46	19.38	0.66	18.11	0.53
Salt and pepper	16.57	0.55	17.09	0.56	16.56	0.56	16.74	0.55
Gaussian white	15.29	0.36	14.92	0.34	15.40	0.37	15.20	0.35
Poisson	26.56	0.82	26.45	0.81	28.19	0.88	27.06	0.84

Fig. 3 illustrates that proposed scheme has quite good performance on extracting digital watermark through visual effect with different types of noise attack. PSNR and SSIM indices results shown in Table 1 and Table 2 confirm the digital watermark steganography capability of proposed scheme in noisy circumstances.

Conclusion

In this Letter, a novel steganography scheme which can protect the copyright is proposed based on Arnold scrambling transform and the extension of SGMCA theory to BSS framework. Experiments prove the effectiveness of proposed scheme. Both visual effect and quantitative results of PSNR & SSIM indices illustrate its good performance on steganography of digital watermark and robustness to several different noise attacks through communication channel.

References

[1] Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding-a survey[J]. Proceedings of the IEEE, 1999, 87(7):1062-1078.

[2] Hang Fang-yuan. Image Scrambling Based on Arnold Transform ing and Implem entation[J]. Journal of Guizhou Universit,2008,25(3):276-279.

[3] Elad M, Starck J L, Querre P, et al. Simultaneous cartoon and texture image inpainting using morphological component analysis (MCA)[J]. Applied & Computational Harmonic Analysis, 2005, 19(3):340-358.

[4] Yu C, Chen X. Speed-up generalized morphological component analysis technology used in remote sensing image inpainting application[J]. Arabian Journal of Geosciences, 2014, 8(3):1-9.

[5] Bobin J, Starck J L, Fadili J, et al. Sparsity and morphological diversity in blind source separation.[J]. Image Processing IEEE Transactions on, 2007, 16(11):2662-2674.

[6] Li Xiang. Study on morphological deconvolution method for dispersive and multi-modes phenomena in ultrasonic guided waves[D].University of electronic science and technology of China, 2013.

[7] Wang Z, Bovik A C, Sheikh H R, et al. Image quality assessment: from error visibility to structural similarity[J]. IEEE Transactions on Image Processing, 2004, 13(4):600 - 612.