A Novel Digital Watermarking Approach against Geomeetical Distortions using DWT and LS-SVM

Hui Chen[1], Fei Long[2] and Zhiyun Duan[3]

[1 2 3]Department of Electronic Information, College of Dianchi, Kunming, China.
Email: yndaxuechenhui_84@163.com

Abstract. This paper proposes a novel algorithm for blind watermarking by applying discrete wavelet transformation and least squares support vector machine into watermark embedding and detection. It is strong against general attacks in the traditional digital watermarking, but difficult to geometric attacks. Firstly, discrete wavelet transformation is performed on coefficient block and watermark image is embedded. Subsequently, the trained least squares support vector machine is employed to extract the watermark blindly. Experimental results confirm that the proposed scheme is not only robust against common attacks such as noise, filter and crop, but also robust against geometrical distortions.

1. Introduction

With the development of new digital technology, it becomes easy for people to access the multimedia data, such as music, pictures, e-books and video. Therefore, the protection of intellectual property rights is becoming increasingly important. It is a technology that to embed some information into digital carrier, and not affectted the value of the host carrier [1]. Therefore, it is difficult to be detected or modified again, but it could be recognized by the producer. In recent years, digital watermarking based on DWT is becoming more and more popular since it makes use of non-fixed orthogonal bases which are often used by most of the unitary transformations. It is the first time that Kunder proposed the DWT (Discrcte Wavelet Transform) –based watermarking. First of all, the host image and watermarking are transformed by wavelet transform; subsequently, the watermark of the special stator is embedded in the corresponding image subband; thirdly, the embedded image is obtained by taking inverse wavelet transform. Now the digital watermarking based on DWT is not only be used to the image, but also is a good effect in the speech and video. Moreover, the wavelet transform and the watermarking algorithm based on the space domain have better effects on anti-interference and robustness. Chang [2] proposes a digital watermarking method based on SVD by the singular value decomposition (SVD) of the image matrix, which imbeds the Gauss random sequence and determines the watermarking by the correlation detection. In [3], Zheng proposed a digital watermarking method based on SVD and SVM, A similar method is proposed in [4] to which the optimization objective is the blind watermarking method, in which SVD and SVM are employed for watermark embedding. In the two paper, it is used the characteristics of matrix sparsity to avoid large computation that eigenvalues and eigenvectors in the singular value decomposition, but SVD is insensitive to geometrical deformation and SVM is limitated in geometrical distortions, so the method is worse to resist geometrical distortions . Zhou [5] proposes a geometric distortion digital watermarking algorithm which is implemented with singular value decomposition, it is very novel, but is not good for resisting other attacks, such as noise and JPEG compression.

In the paper, a novel combination of LS-SVM and DWT method is proposed to resist the geometrical distortion. Firstly, the host image is applied into the method of multi-scale wavelet transform and the watermark is employed for Arnold transformation. Since the first singular value in the watermarked image is important, it could not be destroyed. This is an approach to tackle this problem that the intensity of embedding in the first singular value is less than others. Then the singular values in the watermarked image is embedded into the different components which are the last level ones in the discrete wavelet transformation of the host image. In fact, LS-SVM is utilized to memorize the relationship between original coefficients and their watermarked version, which is applied into correcting geometrical distortions using the principal component. It is known that the possible types of errors in regression processing are analyzed, so the watermark is extracted by the correction of watermarked image.

The scheme consists of 3 parts: watermark embedding, LS-SVM training and watermark extraction. Meanwhile, the block diagrams of these 3 parts is shown from Figure 1.

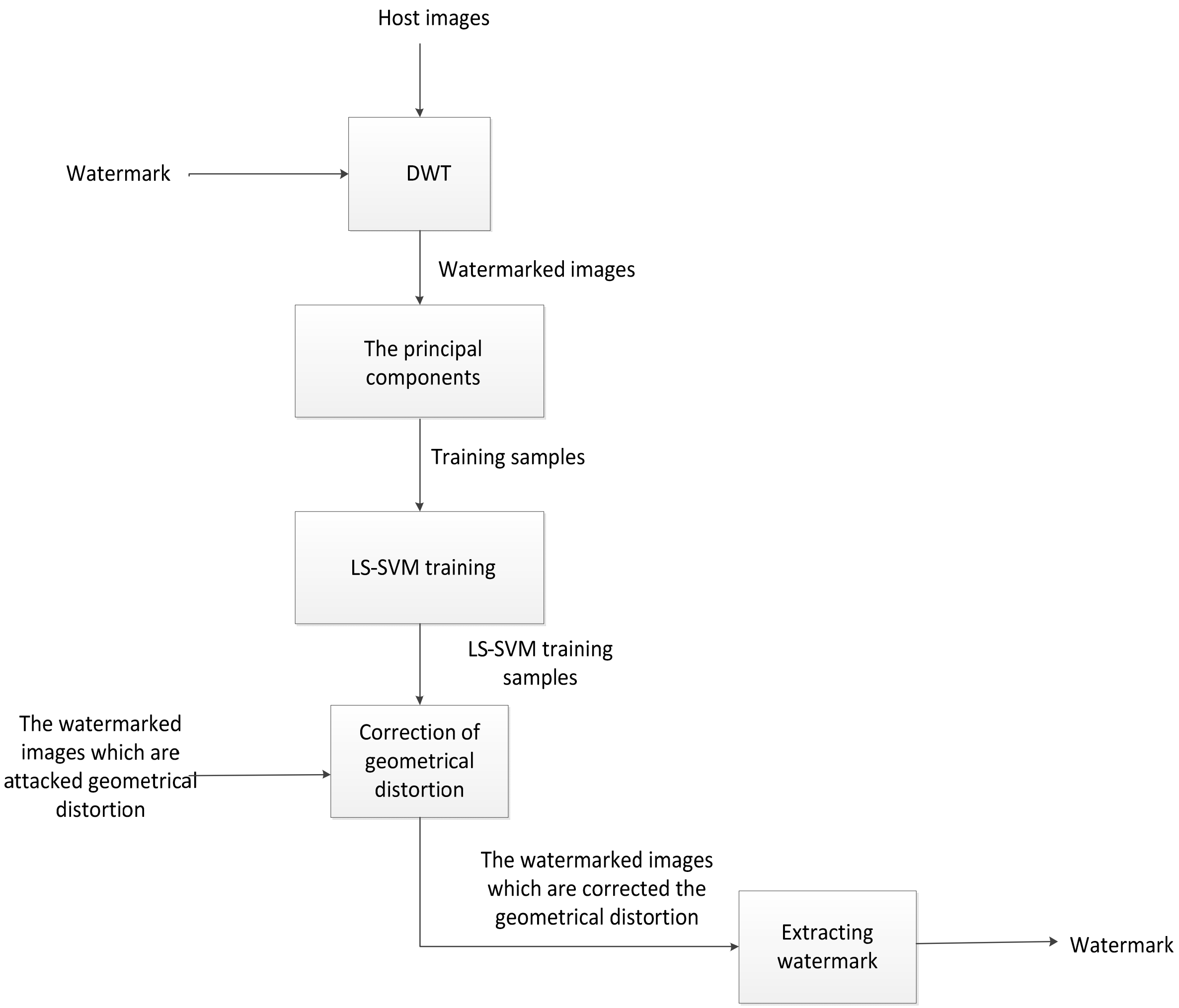
Host images
Watermark
DWT
Watermarked images
The principal components
Training samples
LS-SVM training
LS-SVM training samples
The watermarked images which are attacked geometrical distortion
Correction of geometrical distortion
The watermarked images which are corrected the geometrical distortion
Extracting watermark
Watermark

Figure 1. The entire process

2. Watermark Embedding Based On Dwt

The basic principle of the digital watermarking embedding algorithm based on DWT which is developed the spatial domain into the frequency domain. Then the watermark is embedded into low frequency coefficient matrix. Finally, the frequency domain is converted into the spatial domain to complete the embedding of the watermark. The specific embedding procedure is as follows:

Step1: The M by M gray scale host image is divided into 8×8 subblocks, and each subblock is transformed by DWT. The matrix is recorded $P(i, j) 1 \le i \le 8, \quad 1 \le j \le 8$, where $P(1,1)$ is DC coefficient and the low frequency coefficients are the other parts of the matrix;

Step2: The N by N binary watermark is employed for Arnold transformation and stored in the order of every two subblocks as one bit, which is embedded in $P(1,3)$ that is the low frequency coefficient of $P(i, j)$ and the new one is recorded as $P^*(1,3)$;

Step3: The process that the watermark is embedded into the low frequency coefficients is as follows [6]:

$$t = P^*(1,3)$$

$$z = \mathrm{mod}(t, N)$$

$$t = \begin{cases} t + N/4 - z & \text{The binary value of the watermark pixel is } 0\, and \quad z < 3N/4 \\ t + 5N/4 - z & \text{The binary value of the watermark pixel is } 0\, and \quad z \geq 3N/4 \\ t + N/4 - z & \text{The binary value of the watermark pixel is } 1\, and \quad z < N/4 \\ t + 3N/4 - z & \text{The binary value of the watermark pixel is } 1\, and \quad z \geq N/4 \end{cases}$$

Step4: The embedded image is transformed into IDWT and sequentially stored back, then it is reconstructed the watermarked image I'.

3. Watermark Extraction Based On Dwt

The digital watermarking extraction algorithm based on DWT is described as follows:

Step1. After the watermarked image is transformed by DWT with 8×8 subblocks, the matrix is recorded $Q(i, j) 1 \leq i \leq 8,\ \ 1 \leq j \leq 8$. If the watermarked image is not attacked, $Q(1,3) = P^*(1,3)$ is ture, or else, the image W can be extracted by the low frequency coefficient $Q(1,3)$ of the revised watermarked image.

Step2. The image W is obtained by the lower frequency coefficient by the following formula [6].

$$t' = Q(1,3)$$

$$z = \mathrm{mod}(t', N)$$

$$W = \begin{cases} 0, & z < N/2 \\ 1, & z \geq N/2 \end{cases}$$

Step3. Perform inverse Arnold transformation on image W and the watermark can be extracted.

4. LS-SVM

Support vector machine (SVM) was introduced by Vapnik which has been successfully used to the problems of linear classification and nonlinear functions, and the goal of SVM is to find the hyperplane that maximizes the minimum distance between any data point, as depicted in reference [7]. In contract with SVM, Least squares support vector machine (LS-SVM) is not only used to solve classification issues but also regression ones, which has as trong adaptiveability. The watermarked images which are attacked geometric distortion would be corrected, and LS-SVM is a common method of geometric correction, as a supervision learning model. This paper proposes the regression analysis to the geometric attack parameters.

In this paper, $K(x, y) = \exp[-|x - y|^{\frac{2}{d^2}}]$ is the kernel function of LS-SVM which is used for regression analysis. The principal components are used for feature extraction. Its basic principle is to build the principal components based on K-L transformation to extract the feature vectors of the M by M watermarked images under geometric attack.The procedure is as follows:

Step1: The n watermarked images under geometric attack are $x = \{x_i, x_i, ..., x_i\} \in R^m$, where $x_i (i = 1,2,...,n)$ is an m-dimensional column vector.The covariance matrix constructed for LS-SVM training samples is $S = \sum_{i=1}^{n} (x_i - \bar{x})(x_i - \bar{x})^T$, where $\bar{x}$ is the mean value of the training samples.

Step2: The r non-zero eigenvalues are solved by the sample covariance matrix S, where $\lambda_j (j = 1,2,...,r)$ is the j-th eigenvalues. Sort by the size of the eigenvalues, i.e $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_r > 0$.

Step3: The eigenvectors corresponding to each eigenvalue are $U_j (j = 1,2,...,r)$, that the first column of the principal components vectors is the former p eigenvectors. U_{11} is called the first principal component, U_{21} is called the second principal component, and so on, U_{p1} is called the p-th principal component.

Since it is required less dimensions of principal component vectors for geometric correction of watermarked images, we select the four low-order principal component vectors which are defined as $(c_1 \quad c_2 \quad c_3 \quad c_4)$ for the feature vectors of training samples. The rotation angle, translation and scaling parameters for regression analysis are defined as $(\theta \quad \mu \quad \alpha)$.

The sets of supposed training sample are defined as $E^t (t = 1,2,..., n)$, $E^p (p = 1,2,..., n)$, $E^q (q = 1,2,..., n)$. Then the LS-SVM model can be referred to as $\Omega_t = (c_1^t, c_2^t, c_3^t, c_4^t, \theta^t)$, $\Omega_p = (c_1^p, c_2^p, c_3^p, c_4^p, \mu^p)$, $\Omega_q = (c_1^q, c_2^q, c_3^q, c_4^q, \alpha^q)$.

5. Simulations

In our simulations, three host images and one watermark are tested. Three host images with sizes 256×256, are shown from Figure 2 a–c, referred to as “Lena”, “Woman”, “Camera”, respectively and one watermark image with size 16×16 is shown in Figure 3. Three watermarked images are shown from Figure 2 d–f.

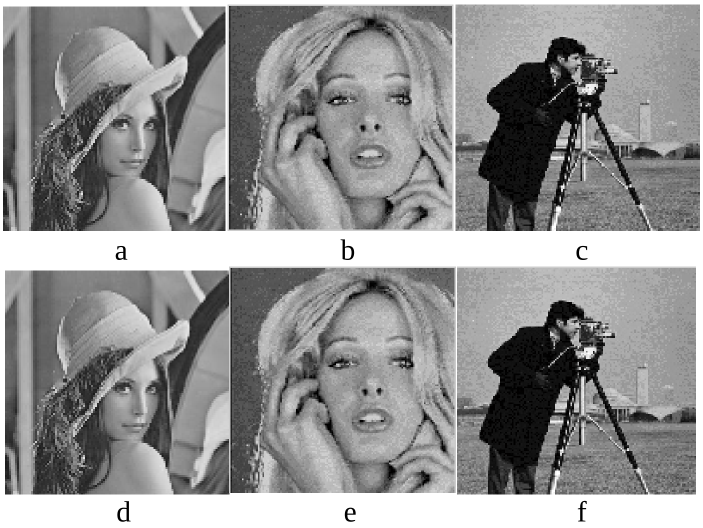

Figure 2. a~c The host images of Lena, Woman, Camera,

d~f The watermarked images of Lena, Woman, Camera.

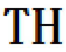

Figure 3. The watermark image

Peak signal-to-noise ratio (PSNR) between original host image and watermarked image is measured by Eq. (1).

$$PSNR = 10 \times \lg \frac{mn \times \max(I_{ij}^{2})}{\sum_{i=1}^{m} \sum_{j=1}^{n} [I_{ij} - \hat{I}_{ij}]^2} \tag{1}$$

Where I_{ij} and $\hat{I}_{ij}$ refer to the host image and watermarked image; m and n refer to the width and length of host image, respectively. The peak signal-to-noise ratio of the above three watermarked images that are also used in references [3] and [4] is shown in table 1:

Table 1. The peak signal-to-noise ratio of the watermarked images (PSNR)

	The algorithm of this paper	The algorithm of scheme [3]	The algorithm of scheme [4]
Lena	38.1641	36.2713	37.0976
Woman	39.3471	40.1547	39.1654
Camera	37.2498	37.6983	35.6945

Normalized correlation (NC) between original watermark and extracted watermark is computed by Eq. (2).

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W_{ij} \times \hat{W}_{ij}}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W_{ij}^{2}}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} \hat{W}_{ij}^{2}}} \tag{2}$$

Where W_{ij} is the original watermark and $\hat{W}_{ij}$ is the extracted watermark; m and n denote the equal width and length of watermark, respectively. After the common and geometric attack on the embedded image of “Lena”, the algorithm in this paper is used to extract the watermark and calculate the normalized correlation, as shown in table 2 and table 3:

Table 2. The watermark detection results for common image processing operations (NC).

Common attack	The algorithm of this paper	The algorithm of scheme [3]	The algorithm of scheme [4]
Median filtering	0.82789	0.81098	0.69287
Salt-and-pepper noise	0.83319	0.76980	0.85098
Sharpening (32,32)	0.82678	0.74398	0.78093

Table 3. The watermark detection results for geometric distortions (NC).

Geometric attack	The algorithm of this paper	The algorithm of scheme [3]	The algorithm of scheme [4]
Rotation 45^0	0.86676	0.71865	0.79231
Translation (H 20,V 20)	0.88653	0.72025	0.76256

From Table 1, PSNR of the algorithm in this paper is close to 40dB, which meets the requirement and the watermark is hidden. In Table 2and Table 3, It is the high quality of the extracted watermark by this algorithm, and the NC value is close to 1.

6. Conclusion

With the improvement of digital watermarking, the algorithm based on LS-SVM in this paper could correct the coefficient that are inaccurate in the digital watermarking under geometric attack of rotation, translation and scaling. Experiments show that our algorithm is improved the robustness and PSNR of digital watermarking.

7. References

[1] Zhang weiping.Modeling and control of switch converter [M].Beijing: China Electric Power Press, 2006, pp15-88.

[2]C.C.Chang, P.Tsai, C.C.Lin, SVD-based digital image watermarking scheme, PatternRecognit. Lett. 26 (10) (2005) 1577-1586.

[3]Pan-PanZheng, JunFeng, ZhanLi, Ming-quanZhou, A novel SVD and SVM combination algorithm for blind watermarking, Neurocomputing, 142 (2014) 520-528.

[4] Hong-yingYang, Pan-panNiu, Robust image watermarking approach using polar harmonic transforms based geometric correction, Neurocomputing, 174 (2016) 627-642.

[5]Xiang Yang Wang, Hong Ying Yang, Chang Ying Cui, An SVM-based robust digital image watermarking against desynchronization attacks, IEEE Transactions on Singal Processing 88 (2008) 2193-2205.

[6]S. A. Martucci, Symmetric convolution and the discrete sine and cosine transforms, IEEE Trans. Sig. Processing 42 (1994), 1038-1051.

[7] V. Vapnik, The Nature of Statistical Learning Theory, Springer, New York, 1995.