future internet

MDPI

Article

Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection

Yunpeng Zhang, Chengyou Wang, Xiaoli Wang * and Min Wang

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China; zhyp@mail.sdu.edu.cn (Y.Z.); wangchengyou@sdu.edu.cn (C.W.); wangmin305026@163.com (M.W.)
* Correspondence: wxl@sdu.edu.cn; Tel.: +86-631-568-8338

Academic Editor: Luis Javier Garcia Villalba
Received: 8 March 2017; Accepted: 14 April 2017; Published: 19 April 2017

Abstract: Watermarking techniques can be applied in digital images to maintain the authenticity and integrity for copyright protection. In this paper, scale-invariant feature transform (SIFT) is combined with local digital watermarking and a digital watermarking algorithm based on SIFT, singular value decomposition (SVD), and all phase biorthogonal transform (APBT) is proposed. It describes the generation process of the SIFT algorithm in detail and obtains a series of scale-invariant feature points. A large amount of candidate feature points are selected to obtain the neighborhood which can be used to embed the watermark. For these selected feature points, block-based APBT is carried out on their neighborhoods. Moreover, a coefficients matrix of certain APBT coefficients is generated for SVD to embed the encrypted watermark. Experimental results demonstrate that the proposed watermarking algorithm has stronger robustness than some previous schemes. In addition, APBT-based digital watermarking algorithm has good imperceptibility and is more robust to different combinations of attacks, which can be applied for the purpose of copyright protection.

Keywords: image watermarking; scale-invariant feature transform (SIFT); all phase biorthogonal transform (APBT); singular value decomposition (SVD); robustness; copyright protection

1. Introduction

Since the 1990s, information hiding technology has become a major research focus in the field of information technology. The purpose of information hiding is to embed hidden data in digital media, such as image, audio, video, and so on. With the development of related technologies, information hiding has become an independent discipline, and its coverage is also expanding. According to the purpose of hiding information and technical requirements, invisibility, robustness, undetectability, security [1], and other attributes are all distinctive features of information hiding technology.

As digital media can be easily copied, altered, and illegally distributed, copyright protection of digital media has aroused increasingly widespread attention. How to protect the integrity and authenticity of digital media becomes urgent and important. Thus, digital signature [2] and digital watermarking [3] have been proposed for data hiding to solve this problem. Due to its superior performance, digital watermarking is applied as an effective method to solve the image's copyright issue. According to different functions, digital watermarking can be classified into three types, containing robust watermarking, fragile watermarking, and semi-fragile watermarking. Robust watermarking can resist all kinds of attacks and common processing, which is applied for copyright protection. Fragile watermarking is sensitive to attacks, including malicious tampering and common processing. Combining advantages of the two above watermarking methods, semi-fragile watermarking is proposed to distinguish malicious tampering from non-malicious modification with the certain ability of resisting common processing. According to the domain where the watermark is embedded, two types of digital watermarking techniques can be defined [4,5]: spatial domain

watermarking [6], and frequency or transform domain watermarking [7]. Spatial domain methods modify the pixel value of the digital image directly to embed the watermark. The least significant bit (LSB) algorithm is the common and simplest algorithm applied in spatial watermarking schemes [8], embedding the watermark information into the LSB or multiple bit layers. Correspondingly, frequency domain methods embed the watermark information by modifying transform coefficients of the original image. Compared with spatial methods, schemes based on transforms have better imperceptibility and robustness. Discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete sine transform (DST), and singular value decomposition (SVD) [9] are common transforms applied in frequency domain watermarking. Moreover, other special transforms, such as redundant DWT (RDWT) [10], fractional wavelet transform (FWT) [11], and QR decomposition [12], can be applied for better performance in some certain aspects. In recent years, these transforms are still applied widely in the watermarking field. For example, Rasti et al. [12] proposed a robust color video watermarking scheme based on QR decomposition and entropy analysis, embedding the watermark into the block selected by entropy analysis. The selected block is performed by DWT, Chirp-Z transform (CZT), QR decomposition, and SVD for watermark embedding. In [13], Cheng et al. proposed a robust watermarking with the combination of DWT and DCT. In the embedding process, the HL_2 sub-band coefficient is divided into 4×4 blocks after decomposing the cover image by two-level DWT. Then, the DCT is performed for each block. According to the watermark bit, two pseudo-random sequences are embedded into the middle band coefficients of DCT. Besides, Guo et al. [14] proposed a robust watermarking scheme based on DCT and DWT in the encrypted domain to improve the robustness, using an image splitting method to embed the watermark in the low-middle frequency coefficients. Nguyen et al. [15] proposed a fragile watermarking for image authentication in the wavelet domain, where the authentication code is embedded into the two-level low frequency sub-band. In [16], Martino and Sessa introduced a fragile watermarking tampering detection with compressed images based on a fuzzy transform, which is applied to compress each block. Besides, fuzzy c-means clustering technique is proposed to form the relationship between image blocks, and this method achieves more accurate tampering detection and localization. Lin and Tsay [17] presented a passive approach for tampering detection and location in video sequences with camera motion, which is based on spatio-temporal coherence analysis.

The scale-invariant feature transform (SIFT) [18] is a classical algorithm for interest points detection, as well as local features description, which has three advantages: (1) the number of extracted feature points or keypoints is significant with appropriate parameter settings; (2) the image feature extracted by SIFT has great uniqueness for accurate matching; and (3) SIFT features have better invariance ability on rotation, scaling, and translation. Owing to its efficiency [19], SIFT algorithm is widely used in the field of image processing to match two images, locate the position, and recognize objects. Moreover, SIFT provides good performance of watermarking schemes in recent years. Lee et al. [20] firstly proposed a novel image watermarking scheme using local invariant features, and embedded the watermark into circular patches generated by SIFT. In [21], Lyu et al. proposed an image watermarking scheme based on SIFT and DWT, and applied the DWT on the selected SIFT areas. Thorat and Jadhav [22] proposed an anti-geometric attack watermarking scheme based on integer wavelet transform (IWT) and SIFT, where feature points in red components of the image are extracted by SIFT, and blue and green components are performed by IWT to extract low frequency coefficients for watermark embedding. Luo et al. [23] presented an adaptive robust watermarking scheme based on discrete Fourier transform (DFT) and SIFT to deal with the synchronization errors. Pham et al. [24] proposed a robust SIFT and DCT-based watermarking scheme, embedding the watermark into the selected feature regions after DCT. In [25], Zhang and Tang introduced an SVD and SIFT-based watermarking algorithm to solve the synchronization problem, where SIFT is used for watermarking resynchronization.

Owing to the robustness feature of SIFT and SVD, as well as better concentration of all phase biorthogonal transform (APBT) in low frequencies, we propose the idea of combining local digital watermarking with SIFT, SVD, and APBT, and make comparisons between previous watermarking

schemes and the proposed watermarking algorithm in this paper. The purpose of this paper is to propose a robust watermarking algorithm with better imperceptibility and stronger robustness for copyright protection.

The remainder of this paper is organized as follows. Section 2 introduces the related work. Section 3 describes the proposed algorithm in detail. Experimental results and analyses are presented in Section 4. Conclusions and future works are given finally in Section 5.

2. Related Work

2.1. Digital Watermarking

The purpose of digital watermarking is to embed obvious information into digital data. The embedded symbol is usually invisible or difficult to detect, but it can be detected or extracted by certain extraction algorithms. The watermark is hidden in the original data as an integral part of it, and general framework of digital watermarking technology is shown in Figure 1.

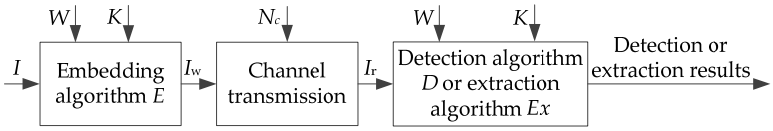

Figure 1. General framework of digital watermarking.

The digital watermark W is combined with the certain key K, which is embedded into original signal I by the embedding method E, generating the watermarked signal I_{w}. In the transmission, owing to the interference of noise N_{c}, the watermarked signal I_{w} can be transformed into I_{r}, and the received signal I_{r} can be evaluated or extracted by applying the detection algorithm D or extraction algorithm Ex.

2.2. APBT

APBT [26] is an improved transform firstly proposed by Hou et al. which can be applied in the field of image processing, such as image compression, image denoising, image demosaicking, and so on [27]. In practice, owing to the fact that APBT has better energy concentration in low frequencies and attenuation characteristics in high frequencies, it has better applications in image processing. Suppose that $\boldsymbol{X}$ is the data of a $B \times B$ image block, and $\boldsymbol{V}$ represents the APBT matrix with the size of $B \times B$, respectively, the transform coefficients block $\boldsymbol{Y}$ after two-dimensional APBT transform can be denoted by:

$$\boldsymbol{Y} = \boldsymbol{V}\boldsymbol{X}\boldsymbol{V}^{\mathrm{T}}, \tag{1}$$

where $\boldsymbol{V}^{\mathrm{T}}$ is the transpose matrix of $\boldsymbol{V}$. In the contrary, we use:

$$\boldsymbol{X} = \boldsymbol{V}^{-1}\boldsymbol{Y}(\boldsymbol{V}^{-1})^{\mathrm{T}}, \tag{2}$$

to reconstruct the image, and $\boldsymbol{V}^{-1}$ is the inverse matrix of $\boldsymbol{V}$.

When transform matrix $\boldsymbol{V}$ is set as the different forms as Equations (3) and (4) separately, the corresponding transforms can be defined as all phase discrete cosine biorthogonal transform (APDCBT) and all phase inverse discrete cosine biorthogonal transform (APIDCBT), respectively.

$$\boldsymbol{V}_1(p,q) = \begin{cases} \frac{B-p}{B^2}, & p = 0,1,\cdots,B-1, q = 0, \\ \frac{1}{B^2}\left[(B-p)\cos\frac{pq\pi}{B} - \csc\frac{q\pi}{B}\sin\frac{pq\pi}{B}\right], & p = 0,1,\cdots,B-1, q = 1,2,\cdots,B-1, \end{cases} \tag{3}$$

$$\boldsymbol{V}_2(p,q) = \begin{cases} \frac{1}{B}, & p = 0,\ q = 0,1,\cdots,B-1, \\ \frac{B-p+\sqrt{2}-1}{B^2}\cos\frac{p(2q+1)\pi}{B}, & p = 0,1,\cdots,B-1,\ q = 1,2,\cdots,B-1. \end{cases} \tag{4}$$

2.3. SIFT Algorithm

The SIFT algorithm was proposed by Lowe [28] to extract the local scale-invariant feature points, which are used for matching two related images. Generation steps of SIFT feature descriptors are described in the following.

The first step is scale-space selection. The basic idea of the scale-space approach is to introduce a scale parameter into the visual information processing model and obtain visual processing information at different scales by continuously changing scale parameters. Then, the information is integrated to explore the essential characteristics of the image. The Gaussian convolution kernel [29] is the only linear kernel to achieve the scale transformation, and the scale-space kernel f_{out} can be defined as:

$$f_{\text{out}} = K_{\text{n}} * f_{\text{in}}, \tag{5}$$

where K_{n} is the kernel, f_{in} is the input signal, and $*$ represents the convolution operation.

Scale-space $S(x, y, \sigma)$ of image $I(x, y)$ is shown as:

$$S(x, y, \sigma) = G(x, y, \sigma) * I(x, y), \tag{6}$$

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} \mathrm{e}^{-(x^2+y^2)/2\sigma^2}, \tag{7}$$

where $G(x, y, \sigma)$ is the scale variable Gaussian function, (x, y) are the spatial coordinates, and σ is the scale-space factor, which decides the smoothness of the image. A large value of σ represents a smooth image with overview feature, while a small value of σ describes an abundant image with detailed feature. To effectively detect stable points in the scale-space, Lowe [28] proposed the difference of Gaussian (DOG) scale-space, presented as:

$$D(x, y, \sigma) = [G(x, y, k\sigma) - G(x, y, \sigma)] * I(x, y) = S(x, y, k\sigma) - S(x, y, \sigma), \tag{8}$$

where $I(x, y)$ is the input image, k is the multiple between two neighboring scale-spaces, and $*$ represents the convolution operation. To detect the local maxima and minima of $D(x, y, \sigma)$, each point is compared with its eight neighbors in the current image and nine neighbors in the scale above and below. With the help of the DOG scale-space image, all extreme points can be detected as feature points.

The second step is to locate feature points, aiming at orientating the location of feature points precisely. In this way, a large number of extreme points are obtained. However, not all extreme points are feature points. Therefore, a suitable method is needed to eliminate some points.

The third step is feature point orientation assignment, and the purpose is to achieve the SIFT features of rotation invariance. For scaling the smoothed image I_{L}, the central derivative of I_{L} at each feature point can be computed. The scale and orientation at feature point (x, y) can be calculated by:

$$\begin{cases} \theta(x, y) = \tan^{-1} 2\{[I_{\text{L}}(x, y+1) - I_{\text{L}}(x, y-1)]/[I_{\text{L}}(x+1, y) - I_{\text{L}}(x-1, y)]\} \\ g(x, y) = \sqrt{[I_{\text{L}}(x+1, y) - I_{\text{L}}(x-1, y)]^2 + [I_{\text{L}}(x, y+1) - I_{\text{L}}(x, y-1)]^2} \end{cases}, \tag{9}$$

where $\theta(x, y)$ is the orientation of the gradient, and $g(x, y)$ is the magnitude.

After obtaining the gradient direction and amplitude, the gradient direction of feature points can be determined by a gradient direction histogram. The peak represents the main direction. In the gradient direction histogram, when another peak value equals 80% of the main peak's value, this direction should be set as the auxiliary direction of this feature point. The direction matching has been completed with the location, orientation, and scale, and this step is to find the local image descriptor of the feature points.

This completes all steps of the SIFT algorithm.

3. The Proposed Algorithm

In this section, a novel watermarking algorithm based on SIFT, SVD, and APBT is proposed and compared with previous watermarking schemes.

3.1. Preparation before Embedding

Although a large number of feature points are obtained by SIFT, some feature points are still not suitable for watermark information embedding and extraction in terms of scale and orientation. Therefore, feature points should be screened and improved before embedding operation.

In this section, the Airplane image is chosen to embed the watermark for representation. Figure 2 represents the obtained information of feature points after SIFT. The length of the blue arrow in the host image represents the scale, pointing to the direction of feature points, and 2050 feature points are picked out by SIFT, in total.

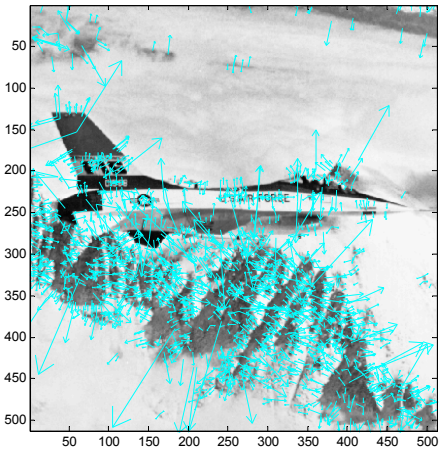

Figure 2. Feature points of the host image by the SIFT algorithm.

Since the scale range of initially obtained feature points are 0–50, points with larger or smaller scales may not be easily detected or successfully matched. Therefore, a certain scale range of points should be selected as candidate feature points, and points whose scale is between 2.3 and 8 are selected as feature points. Then, the 8×8 size of the neighborhood is chosen for each feature point to define feature regions for following operations. Additionally, feature points which are beyond the image boundary and have overlapping neighborhoods with others should be eliminated. Finally, feature points for embedding watermarks are obtained, as shown in Figure 3, where feature points are located in the center of the rectangles.

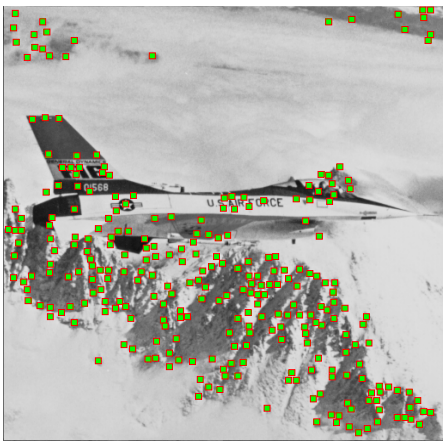

Figure 3. Ultimate feature points for watermark embedding.

3.2. Watermark Embedding

Figure 4 shows the procedure of watermarking embedding based on SIFT, SVD, and APBT.

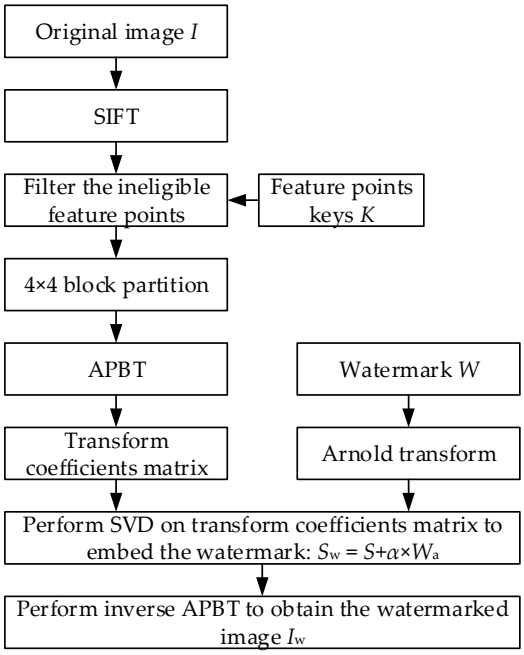

Figure 4. Watermark embedding procedure of the proposed scheme.

Step 1. The host image I is operated by SIFT, and feature points, as well as their parameters of orientation, scaling, and location, can be obtained. All feature points should be screened in the next step.

Step 2. According to the rules demonstrated in Section 3.1, scales of feature points should be restricted into a certain range, and ultimate feature points can be selected for embedding. Thus, coordinates of final feature points are saved as keys K.

Step 3. To improve the watermark security, Arnold transform is performed on watermark W on the basis of Equation (10):

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{pmatrix} 1 & b \\ a & ab+1 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod(N), \tag{10}$$

where (x_i, y_i) are original coordinates of the image pixel, and (x_{i+1}, y_{i+1}) are scrambled coordinates. a, b, and N are positive integers. Additionally, mod means modulo operation, and N denotes the width of image matrix. After the Arnold transform, the watermark matrix will be encrypted as W_a.

Step 4. The host image is divided into 4×4 blocks, and APBT is performed on each block. The first four APBT coefficients at the positions of (1, 1), (1, 2), (2, 1), and (3, 1) are selected according to the zig-zag sequence to form a new coefficients matrix M_c at the location of (1, 1), (1, 2), (2, 1), and (3, 1) separately in M_c. After all blocks having been operated, this step is completed.

Step 5. SVD is performed on coefficients matrix to obtain matrix S of singular values, as well as two orthogonal matrices, U and V. The encrypted watermark W_a is embedded into singular values of the coefficients matrix according to Equations (11) and (12):

$$M_c = USV^T, \tag{11}$$

$$S_w = S + \alpha \times W_a, \tag{12}$$

where α is the scaling factor, determining the performance of the watermarking scheme in robustness and imperceptibility. $\times$ represents the product of α and W_a.

Step 6. SVD is performed on the S_w in Equation (12) again, which is illustrated by:

$$S_w = U_w S_{ww} (V_w)^T. \tag{13}$$

where S_{ww} is the singular values matrix of S_w. Additionally, U_w and V_w are two orthogonal matrices.

Step 7. The watermarked coefficients matrix M_{cw} is generated by S_{ww}, U, and V:

$$M_{cw} = U S_{ww} V^T. \tag{14}$$

Step 8. In converse to the Step 4, certain values in the coefficients matrix M_{cw} are selected to form the watermarked blocks.

Step 9. The inverse APBT is performed to obtain the watermarked image I_w.

3.3. Watermarking Extraction

The procedure of watermark embedding based on SIFT, SVD, and APBT is shown in Figure 5.

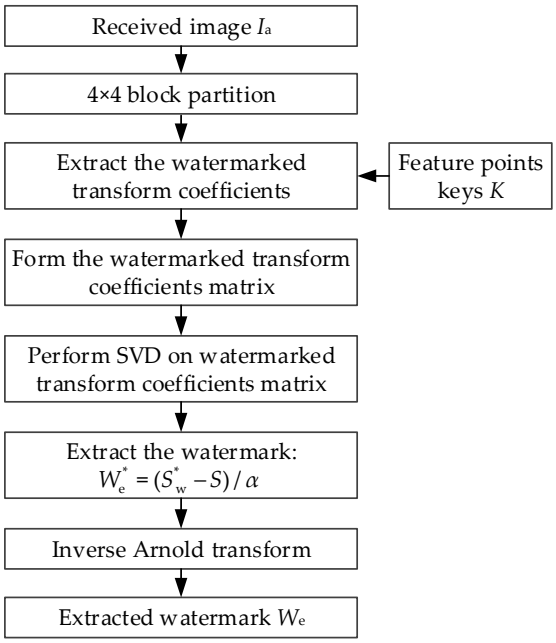

Figure 5. Watermark extraction procedure of the proposed scheme.

Step 1. 4×4 block-based APBT is carried out on the received image after attacks I_a and the first four coefficients of each block are picked out according to the zig-zag sequence.

Step 2. According to keys K, all feature points are performed by Step 1 to obtain the received watermarked coefficients matrix M_{cw}^*. To differentiate matrix in Section 3.2, superscript $*$ is noted for received matrices.

Step 3. SVD is performed on M_{cw}^* using Equation (15), and S_{ww}^* is recorded for the next step:

$$M_{cw}^* = U^* S_{ww}^* (V^*)^T. \tag{15}$$

Step 4. S_w^* is retrieved by Equation (16):

$$S_w^* = U_w S_{ww}^* (V_w)^T. \tag{16}$$

Step 5. The extracted watermark is generated for coefficients matrix M_{cw}^* in Step 3, which is shown in Equation (17):

$$W_e^* = (S_w^* - S)/\alpha. \tag{17}$$

Step 6. The inverse Arnold transform is performed to extract the watermark W_e.

This completes the watermark extraction process.

4. Experimental Results and Comparative Analyses

In this section, performances in terms of the watermark's robustness and the imperceptibility of the proposed method are given and analyzed. This scheme is tested on images 512 × 512 pixels in size, and the watermark sizes applied in this scheme are 64 × 64 and 32 × 32 pixels, respectively. Moreover, to balance the imperceptibility and robustness of the proposed algorithm, the scaling factor α is set to 5. The execution time is calculated from image reading to watermark extraction. The algorithm is tested on MATLAB R2014a (MathWorks, Natick, MA, USA) with an Intel (R) Core (TM) i3-2100 3.10 GHz CPU (Intel, Santa Clara, TX, USA), 4 GB memory computer.

4.1. Performance Evaluation Indexes

After the watermark embedding, compared with the original image, the quality of the watermarked image will be reduced. Peak signal-to-noise ratio (PSNR) is an important objective quality evaluation index adopted in most watermarking methods to evaluate the watermark's imperceptibility. For an image with size of $M \times N$, PSNR is defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2 MN}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - I_w(i,j)]^2}(\mathrm{dB}), \tag{18}$$

where $I(i,j)$ and $I_w(i,j)$ express pixel values in row i and column j of the host image and the watermarked image separately.

The bit error rate (BER) is used to detect the difference between the extracted and original watermarks, which is shown in Equation (19):

$$\mathrm{BER} = \frac{1}{l}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}|W_e(i,j) - W(i,j)|, \tag{19}$$

where $W(i,j)$ and $W_e(i,j)$ show pixel values at a specific location (i,j) in the original watermark and the recovered watermark respectively. l expresses the length of the watermark information derived from the watermark one-dimensional vector, and $m \times n$ is the size of watermark.

The similarity of two images can be evaluated by normalized correlation (NC), which is defined as:

$$\mathrm{NC} = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[W(i,j) \times W_e(i,j)]}{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[W(i,j) \times W(i,j)]}. \tag{20}$$

Higher NC values represent a better quality of the extracted watermark.

4.2. Performance Comparisons

In this section, owing to APDCBT and APIDCBT having similar performance when applied in the proposed algorithm, one of the typical transforms, the APDCBT matrix in APBT theory, is taken to test the performance of the proposed algorithm concretely. To demonstrate applicability of the proposed

algorithm, different images with different entropies are tested in this section, which are shown in Figure 6.

Figure 6. Tested images: (**a**) Airplane; (**b**) Baboon; (**c**) Barbara; (**d**) Bank; (**e**) Elaine; (**f**) Barche; (**g**) Milkdrop; (**h**) Panzer; (**i**) Announcer; (**j**) Vogue; (**k**) Cablecar; (**l**) Canyon; (**m**) Clown; (**n**) Cornfield; (**o**) Frog; (**p**) Fruits.

To give more detailed subjective experimental results, an original image and a watermarked image, as well as a watermarked image and an APDCBT-based extracted watermark are compared in Figure 7. Considering the symmetry and asymmetry of the watermark, logo watermark 1 and letter watermark 2, defined as w_1 and w_2, are applied in this experiment. As Figure 7 shows, the embedded watermark cannot be distinguished by the naked eye, which illustrates that the proposed algorithm achieves good imperceptibility.

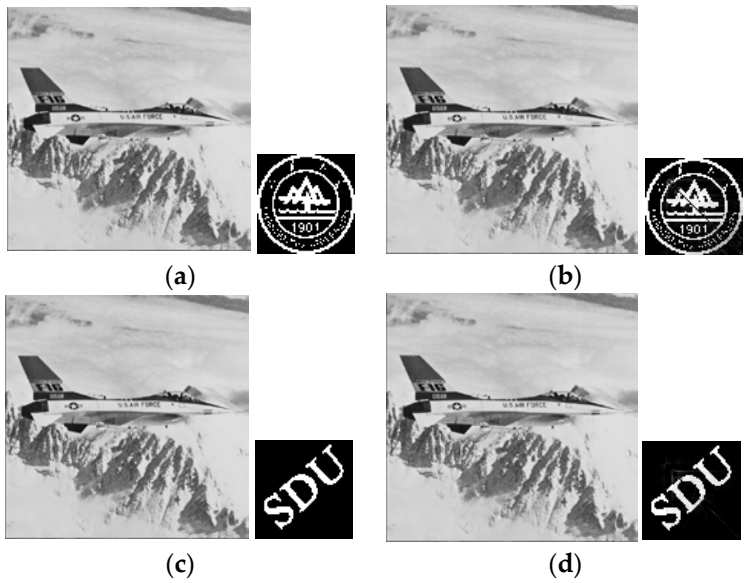

Figure 7. Experimental results on APDCBT-based algorithms: (**a**) original image and w_1; (**b**) watermarked image and extracted w_1 based on APDCBT; (**c**) original image and w_2; (**d**) watermarked image and extracted w_2 based on APDCBT.

Table 1 gives PSNR, NC, and BER values of experimental results. Owing to different entropies of images, the number of selected feature points is different according to Section 3.1. Images with a large number of refined feature points (more than 256), which contains images Airplane, Clown, Cornfield, are tested with a 64 × 64 watermark image. Images with a small number of refined feature points (less than 256), containing images Baboon, Barbara, Bank, Elaine, Barche, Milkdrop, Announcer, Vogue, Cablecar, Canyon, Frog, Fruits, are tested with a 32 × 32 watermark. As can be seen, performance of using symmetrical watermarks and asymmetrical watermarks both have good performance in PSNR.

Table 1. Experimental results on different images with different entropies.

Images		PSNR	NC	BER
Airplane	w_1	90.56	0.9994	0.0008
	w_2	93.28	0.9961	0.0137
Baboon	w_1	79.31	0.9683	0.0156
	w_2	89.76	0.9043	0.0068
Barbara	w_1	91.18	0.9648	0.0176
	w_2	90.27	0.8681	0.0447
Bank	w_1	82.92	0.9577	0.0195
	w_2	91.18	0.9137	0.0317
Elaine	w_1	74.59	0.9401	0.0225
	w_2	77.68	0.7354	0.0680
Barche	w_1	79.55	0.9542	0.0195
	w_2	92.32	0.8772	0.0391
Milkdrop	w_1	78.12	0.9225	0.0273
	w_2	81.05	0.7129	0.0653
Panzer	w_1	78.85	0.9683	0.0146
	w_2	85.78	0.8803	0.0389
Announcer	w_1	76.48	0.8121	0.0957
	w_2	85.50	0.8973	0.0376

Table 1. *Cont.*

Images		PSNR	NC	BER
Vogue	w_1	77.78	0.7928	0.0969
	w_2	83.29	0.8515	0.0434
Cablecar	w_1	86.30	0.8577	0.0770
	w_2	90.28	0.9044	0.0342
Canyon	w_1	85.98	0.8299	0.0784
	w_2	93.29	0.8918	0.0400
Clown	w_1	81.42	0.8208	0.1056
	w_2	87.69	0.8281	0.0489
Cornfield	w_1	86.63	0.8618	0.0853
	w_2	84.19	0.8949	0.0365
Frog	w_1	82.54	0.8270	0.0842
	w_2	85.07	0.8820	0.0430
Fruits	w_1	75.17	0.8879	0.0784
	w_2	81.49	0.9217	0.0291

To give more detailed results, the Airplane image and Shandong University logo are taken as examples for further demonstration. Table 2 indicates the PSNR and NC comparison among methods proposed by Jain et al. [30], Zhang et al. [31], Fzali and Moeini's scheme [32], and the proposed algorithm. In [30], principal components of the watermark are embedded into the host image. In [31], the watermark is scrambled by shuffled SVD (SSVD), and principal components are extracted for watermark embedding. In [32], the watermark is embedded into singular values of the DCT coefficients matrix, which is derived from four segmented sub-images in the DWT domain.

Table 2. Comparison of watermarking algorithms based on APDCBT and previous schemes under different attacks.

Different Indexes	Jain et al. [30]	Zhang et al. [31]	Fzali and Moeini [32]	APDCBT
PSNR (dB)	20.98	39.75	56.42	90.56
Execution Time (s)	1.10	2.43	3.46	6.07
Gaussian Noise (0, 0.01)	0.9695	0.8016	0.9897	0.9983
Salt and Pepper Noise (0.01)	0.9157	0.8925	0.9842	0.9923
JPEG Compression (QF = 50)	0.9877	0.9850	0.9865	0.9830
JPEG Compression (QF = 100)	0.9960	0.9984	0.9999	0.9838
Sparse Region Cropping (100 × 100)	0.8236	0.9236	0.9999	0.9841
Sparse Region Cropping (256 × 256)	-	0.8187	0.9602	0.9821
Dense Region Cropping (100 × 100)	0.6589	0.9255	0.9804	0.9847
Dense Region Cropping (256 × 256)	-	0.8182	0.9682	0.9881

As can be seen in Table 2, owing to the large number of feature points, the watermark information is embedded into the points neighborhood sparsely, which leads to a high PSNR value of the proposed scheme. Due to the block partition in the algorithm, the execution time will be higher. Additionally, the proposed watermarking method has better performance than previous watermarking schemes under some common image attacks. In [32], the host image is divided into four sub-images manually for watermark embedding, resulting in better robustness to JPEG compression.

Moreover, the watermarked image will suffer various types of attacks in the transmission procedures. The performance of the APDCBT-based algorithm is presented in Figure 8, in which (a–f) are watermarked images and extracted watermarks based on APDCBT after five types of attacks: Gaussian noise (0, 0.01), salt and pepper noise (0.01), JPEG compression (QF = 100), cropping the sparse region (100 × 100), and cropping the dense region (100 × 100), which are labeled as 2 to 6, respectively. Furthermore, the result with no attack is labeled as 1.

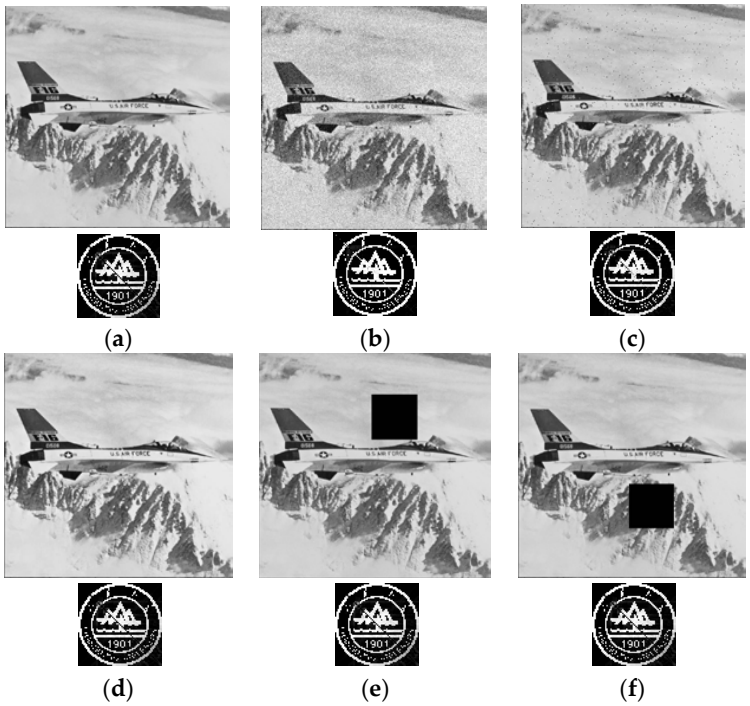

Figure 8. Watermarked images and extracted watermarks based on APDCBT under five types of attacks: (**a**) no attack; (**b**) Gaussian noise (0, 0.01); (**c**) salt and pepper noise (0.01); (**d**) JPEG compression (QF = 100); (**e**) cropping the sparse region (100 × 100); (**f**) cropping the dense region (100 × 100).

Figure 9 shows watermarked images and extracted watermarks in the APDCBT-based watermarking scheme under combinations of the above attacks. Both Figures 8 and 9 demonstrate that the proposed watermarking scheme can extract the watermark with high quality, which can also suggest robustness of the proposed method.

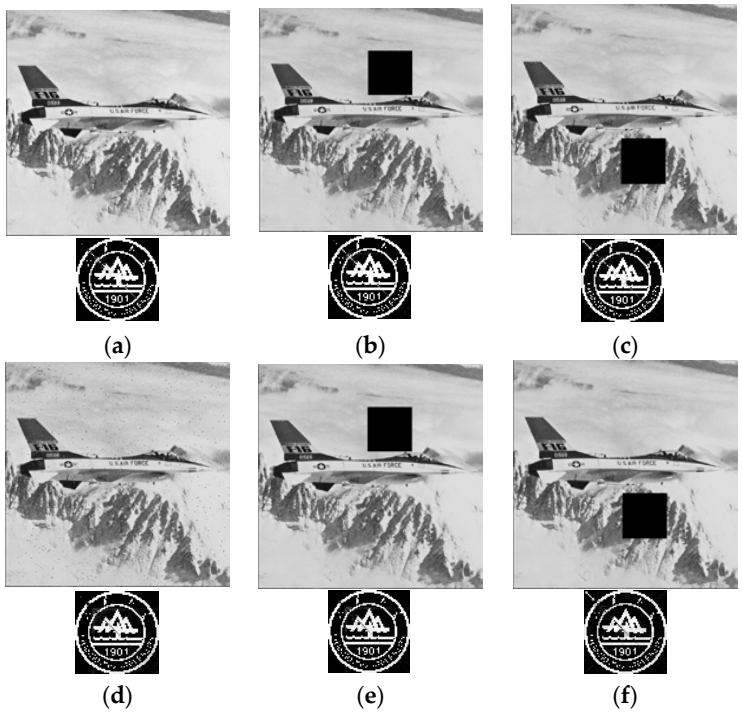

Figure 9. *Cont.*

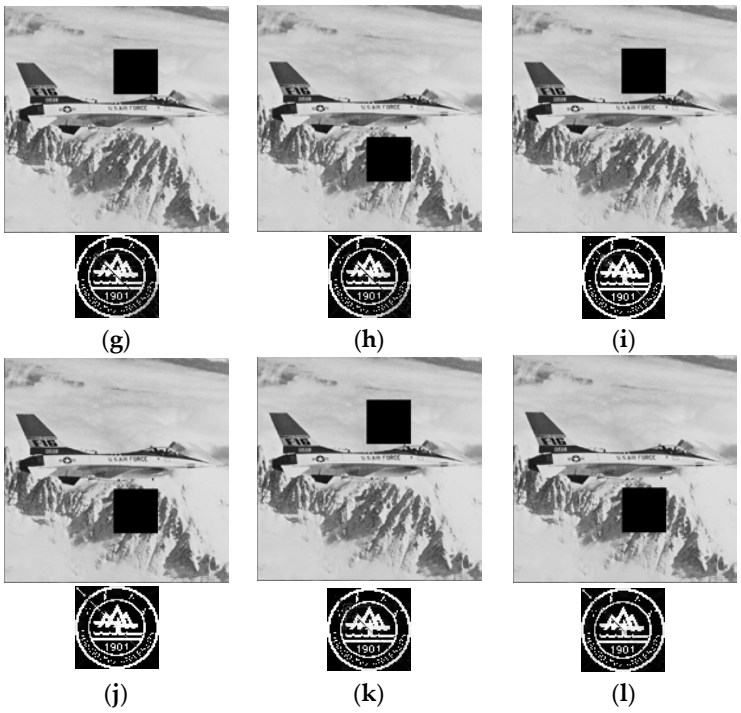

Figure 9. APDCBT-based watermarked images and extracted watermarks under combinations of different attacks: (**a**) 2 and 4; (**b**) 2 and 5; (**c**) 2 and 6; (**d**) 3 and 4; (**e**) 3 and 5; (**f**) 3 and 6; (**g**) 4 and 5; (**h**) 4 and 6; (**i**) 2, 4, and 5; (**j**) 2, 4, and 6; (**k**) 3, 4, and 5; (**l**) 3, 4, and 6.

Additionally, Table 3 illustrates the robustness of the proposed algorithm under combinations of different attacks. In terms of BER and NC, the proposed scheme based on APDCBT has excellent performance.

Table 3. Evaluation of the watermarking algorithms based on APDCBT under different combinations of attacks.

Combination of Attacks	BER	NC
1	0.0008	0.9994
2 and 4	0.0061	0.9945
2 and 5	0.0039	0.9974
2 and 6	0.0049	0.9991
3 and 4	0.0046	0.9949
3 and 5	0.0049	0.9949
3 and 6	0.0081	0.9915
4 and 5	0.0088	0.9838
4 and 6	0.0120	0.9847
2, 4, and 5	0.0046	0.9991
2, 4, and 6	0.0046	0.9993
3, 4, and 5	0.0061	0.9889
3, 4, and 6	0.0066	0.9915

5. Conclusions

In this paper, a robust digital image watermarking algorithm based on SIFT, SVD, and APBT is proposed for copyright protection. Detailed introductions about the SIFT algorithm are made, and by combining the SIFT algorithm with the local digital watermark, the watermarking algorithm is proposed. Then, the neighborhood of feature points for embedding can be obtained by filtering beyond the image boundary and in the overlapping neighborhood. The block-based APBT is carried out on the

neighborhood, respectively, to obtain the coefficients matrix for SVD watermark embedding. To make the scheme more secure, the Arnold transform is applied to the watermark.

Experimental results show that our proposed method has better performance in robustness and imperceptibility. For further work, we will continue to focus on the improved algorithm with small entropies host image and asymmetrical watermarks to achieve better performance on more types of images. Additionally, we will apply the proposed algorithm to color images.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (No. 61201371), the Research Award Fund for Outstanding Young and Middle-Aged Scientists of Shandong Province, China (No. BS2013DX022), and the Natural Science Foundation of Shandong Province, China (No. ZR2015PF004).

Author Contributions: Yunpeng Zhang and Chengyou Wang conceived the algorithm; Yunpeng Zhang and Xiaoli Wang designed the experiments; Yunpeng Zhang and Min Wang performed the experiments; Chengyou Wang and Xiaoli Wang analyzed the results; Yunpeng Zhang drafted the manuscript; and Chengyou Wang revised the manuscript. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Skodras, A.; Christopoulos, C.; Ebrahimi, T. The JPEG 2000 still image compression standard. *IEEE Signal Process. Mag.* **2001**, *18*, 36–58. [CrossRef]
2. Lou, D.C.; Liu, J.L. Fault resilient and compression tolerant digital signature for image authentication. *IEEE Trans. Consum. Electron.* **2000**, *46*, 31–39.
3. Langelaar, G.C.; Setywan, I.; Lagendijk, R.L. Watermarking digital image and video data. *IEEE Signal Process. Mag.* **2000**, *17*, 20–46. [CrossRef]
4. Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. A digital watermark. In Proceedings of the 1st IEEE International Conference on Image Processing, Austin, TX, USA, 13–16 November 1994; pp. 86–90.
5. Mishra, A.; Agarwal, C.; Sharma, A.; Bedi, P. Optimized gray-scale image watermarking using DWT-SVD and Firefly algorithm. *Expert Syst. Appl.* **2014**, *41*, 7858–7867. [CrossRef]
6. Sakthivel, S.M.; Ravi Sankar, A. A real time watermarking of grayscale images without altering its content. In Proceedings of the International Conference on VLSI Systems, Architecture, Technology and Applications, Bengaluru, India, 8–10 January 2015; pp. 1–6.
7. Jin, X.Z. A digital watermarking algorithm based on wavelet transform and Arnold. In Proceedings of the International Conference on Computer Science and Service System, Nanjing, China, 27–29 June 2011; pp. 3806–3809.
8. An, Z.Y.; Liu, H.Y. Research on digital watermark technology based on LSB algorithm. In Proceedings of the 4th International Conference on Computational and Information Sciences, Chongqing, China, 17–19 August 2012; pp. 207–210.
9. Qi, X.J.; Xin, X. A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. *J. Vis. Commun. Image Represent.* **2015**, *30*, 312–327. [CrossRef]
10. Makbol, N.M.; Khoo, B.E. Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU—Int. J. Electron. Commun.* **2013**, *67*, 102–112. [CrossRef]
11. Pujara, C.; Bhardwaj, A.; Gadre, V.M.; Khire, S. Secure watermarking in fractional wavelet domains. *IETE J. Res.* **2007**, *53*, 573–580. [CrossRef]
12. Rasti, P.; Samiei, S.; Agoyi, M.; Escalera, S.; Anbarjafari, G. Robust non-blind color video watermarking using QR decomposition and entropy analysis. *J. Vis. Commun. Image Represent.* **2016**, *38*, 838–847. [CrossRef]
13. Cheng, M.Z.; Yan, L.; Zhou, Y.J.; Min, L. A combined DWT and DCT watermarking scheme optimized using genetic algorithm. *J. Multimed.* **2013**, *8*, 299–305.
14. Guo, J.T.; Zheng, P.J.; Huang, J.W. Secure watermarking scheme against watermark attacks in the encrypted domain. *J. Vis. Commun. Image Represent.* **2015**, *30*, 125–135. [CrossRef]
15. Nguyen, T.S.; Chang, C.C.; Yang, X.Q. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. *AEU—Int. J. Electron. Commun.* **2016**, *70*, 1055–1061. [CrossRef]
16. Martino, F.D.; Sessa, S. Fragile watermarking tamper detection with images compressed by fuzzy transform. *Inf. Sci.* **2012**, *195*, 62–90. [CrossRef]

17. Lin, C.S.; Tsay, J.J. A passive approach for effective detection and localization of region level video forgery with spatio-temproal coherence analysis. *Dig. Investig.* **2014**, *11*, 120–140. [CrossRef]
18. Lowe, D.G. Object recognition from local scale-invariant features. In Proceedings of the 7th IEEE International Conference on Computer Vision, Kerkyra, Greece, 20–27 September 1999; Volume 2, pp. 1150–1157.
19. Mikolajczyk, K.; Schmid, C. A performance evaluation of local descriptors. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Madison, WI, USA, 18–20 June 2003; Volume 2, pp. 257–263.
20. Lee, H.; Kim, H.; Lee, H. Robust image watermarking using local invariant features. *Opt. Eng.* **2006**, *45*, 535–545.
21. Lyu, W.L.; Chang, C.C.; Nguyen, T.S.; Lin, C.C. Image watermarking scheme based on scale-invariant feature transform. *KSII Trans. Int. Inf. Syst.* **2014**, *8*, 3591–3606.
22. Thorat, C.G.; Jadhav, B.D. A blind digital watermark technique for color image based on integer wavelet transform and SIFT. *Proced. Comput. Sci.* **2010**, *2*, 236–241. [CrossRef]
23. Luo, H.J.; Sun, X.M.; Yang, H.F.; Xia, Z.H. A robust image watermarking based on image restoration using SIFT. *Radioengineering* **2011**, *20*, 525–532.
24. Pham, V.Q.; Miyaki, T.; Yamasaki, T.; Aizawa, K. Geometrically invariant object-based watermarking using SIFT feature. In Proceedings of the 14th IEEE International Conference on Image Processing, San Antonio, TX, USA, 16–19 September 2007; Volume 5, pp. 473–476.
25. Zhang, L.; Tang, B. A combination of feature-points-based and SVD-based image watermarking algorithm. In Proceedings of the International Conference on Industrial Control and Electronics Engineering, Xi'an, China, 23–25 August 2012; pp. 1092–1095.
26. Hou, Z.X.; Wang, C.Y.; Yang, A.P. All phase biorthogonal transform and its application in JPEG-like image compression. *Signal Process. Image Commun.* **2009**, *24*, 791–802. [CrossRef]
27. Yang, F.F.; Wang, C.Y.; Huang, W.; Zhou, X. Embedding binary watermark in DC components of all phase discrete cosine biorthogonal transform. *Int. J. Secur. Appl.* **2015**, *9*, 125–136. [CrossRef]
28. Lowe, D.G. Distinctive image features from scale-invariant keypoints. *Int. J. Comput. Vis.* **2004**, *60*, 91–110. [CrossRef]
29. Babaud, J.; Witkin, A.P.; Baudin, M.; Duda, R.O. Uniqueness of the Gaussian kernel for scale-space filtering. *IEEE Trans. Pattern Anal. Mach. Intell.* **1986**, *8*, 26–33. [CrossRef] [PubMed]
30. Jain, C.; Arora, S.; Panigrahi, P.K. A reliable SVD based watermarking scheme. *Comput. Sci. arXiv* **2008**. Available online: https://arxiv.org/pdf/0808.0309.pdf (accessed on 18 April 2017).
31. Zhang, Z.; Wang, C.Y.; Zhou, X. Image watermarking scheme based on DWT-DCT and SSVD. *Int. J. Secur. Appl.* **2016**, *10*, 191–206.
32. Fzali, S.; Moeini, M. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Optik* **2016**, *127*, 964–972. [CrossRef]