future internet

MDPI

Article

A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain

Heng Zhang, Chengyou Wang * and Xiao Zhou

School of Mechanical, Electrical and Information Engineering, Shandong University, Weihai 264209, China; sdwhzh@mail.sdu.edu.cn (H.Z.); zhouxiao@sdu.edu.cn (X.Z.)

* Correspondence: wangchengyou@sdu.edu.cn; Tel.: +86-631-568-8338

Received: 23 June 2017; Accepted: 3 August 2017; Published: 7 August 2017

Abstract: With the development of image processing technology, the copyright protection of digital images has become an urgent problem to be solved. As an effective method, the robust digital watermarking technique emerges at a historic moment. Currently, most robust watermarking schemes are performed in the transform domains, such as the discrete cosine transform (DCT) and singular value decomposition (SVD). Compared with spatial domain watermarking schemes, these methods have achieved good performance, such as better robustness and higher security. However, the computational complexity increases with the use of forward and reverse transforms. In this paper, we analyze the SVD-based watermarking scheme and its impact on the spatial domain. Based on this analysis and the mathematical characteristics of SVD, we present a robust image watermarking scheme where a binary watermark is embedded into the largest singular value of each image block in the spatial domain. Several experiments are conducted to verify the performance of the proposed watermarking scheme. The experimental results show that compared with the existing SVD domain watermarking schemes, our proposed method has maintained good robustness against various attacks. Moreover, it avoids the false positive problem existing in traditional SVD-based watermarking schemes and has lower computational complexity.

Keywords: robust image watermarking; singular value decomposition (SVD); spatial domain; Arnold transform

1. Introduction

With the widespread use of digital products, it becomes more and more convenient for us to obtain and modify digital multimedia. However, a negative effect arises at the same time that the copyright of digital multimedia is suffering from a serious threat. To solve this thorny problem, the robust watermarking technique has been proposed. The basic idea of a robust watermarking scheme is to embed a watermark, which is usually a logo or image, into the host image in advance. On the receiving end, the embedded watermark is extracted to prove the ownership of the received image [1]. For the purpose of copyright protection, the watermark should meet two basic conditions: invisibility and robustness. Invisibility refers to that the embedded watermark cannot be discovered by naked eyes. The image after watermark embedding is basically the same as the original host image. Robustness means that the embedded watermark could be well extracted from the image distorted by various attacks. According to different embedding domains, the digital watermarking schemes can be broadly classified into two categories [2]: spatial domain watermarking and transform domain watermarking. In spatial domain watermarking, the watermark is embedded into the host image by directly modifying the pixel values. This method has low computational cost, and it is easy to implement. However, since the watermark embedding process is performed in the spatial domain, spatial domain watermarking is less secure and it has limited ability in resisting some image processing

attacks. In transform domain watermarking, the watermark is embedded by modulating the transform coefficients of the host image. Compared with the former, it achieves stronger robustness and better visual quality. The most commonly used transforms include the discrete cosine transform (DCT) [3] and the discrete wavelet transform (DWT) [4]. In recent years, singular value decomposition (SVD) has been extensively applied in transform domain watermarking due to its good stability in signal processing. In [5], a classical robust watermarking method based on SVD was proposed by Liu and Tan. In their scheme, the watermark embedding process is completed by adding the watermark to the singular values of the host image directly. The left and right singular vectors generated in the watermark embedding process are stored and used as side information to extract the watermark on the receiving end. However, later research found that this method is subjected to a severe false positive problem [6,7]. A different watermark can be extracted from the watermarked image by using different singular vectors. To resolve this issue, Jain et al. [8] suggested a reliable SVD-based watermarking. Unlike [5], the principal component of the watermark is utilized to adjust the singular values of the host image, and one of the singular vectors is served as side information to extract the watermark. Since the singular vectors still contain a wealth of image information, no one can obtain the watermark without correct side information. Therefore, this method provides an effective solution for the false positive problem. The main drawback of this scheme is that it has much influence on the visual quality of the host image, which cannot be applied in our real lives.

To further improve the performance of the SVD-based watermarking scheme, many hybrid watermarking schemes have been put forward, which combine SVD with DCT, DWT, and other transforms. In [9], Lai and Tsai proposed a DWT-SVD-based watermarking method. In their method, the original image is first decomposed by DWT decomposition, and the singular values of high frequency sub-bands in the horizontal and vertical directions (HL and LH) are modified by the watermark. Gupta and Raval [10] presented a robust watermarking scheme that is based on DWT and singular values replacement. The principal component of the watermark is embedded into the singular values of the diagonal high frequency sub-band (HH). Though it achieves a certain degree of robustness under different attacks, the extracted watermark has poor image quality. In [11], Fazli and Moeini proposed a robust watermarking scheme based on DWT, DCT, and SVD. The host image is segmented into four parts: the up-left part, the up-right part, the bottom-left part, and the bottom-right part. For each part, the DWT followed by the DCT transform is applied. The first two alternating current (AC) coefficients in each DCT coefficient matrix are selected to form a new matrix. At last, a 32×32 binary watermark is embedded into the AC coefficients matrix in the SVD domain. This method provides a high robustness for image cropping attack, since the four parts in different directions are embedded by the same watermark. However, at the same time, this also brings a high computational cost compared with other algorithms. By using the redundancy of redundant discrete wavelet transform (RDWT), Makbol and Khoo [12] proposed an RDWT and SVD based watermarking scheme. However, in [13], Guo and Prasetyo presented three vulnerable attacks and proved that the watermarking scheme in [12] is not secure for image copyright protection. To avoid the false positive problem, Guo and Prasetyo [14] proposed a DWT and shuffled SVD (SSVD) [15] based robust watermarking scheme. Instead of embedding the whole watermark, the principal component of the watermark is embedded into the largest singular value of each block. The experimental results show that the quality of the reconstructed watermark is greatly improved due to the use of SSVD. D. Singh and S. K. Singh [16] proposed a DWT-SVD and DCT based robust watermarking method, which provided another solution for the false positive problem. In their method, a grayscale watermark image is first split into two planes called the most significant bits (MSBs) plane and the least significant bits (LSBs) plane. Then, the DCT coefficients of these two planes are embedded into the middle singular values of each 4×4 block in HL and LH sub-bands. Compared with the traditional SVD-based watermarking scheme, the hybrid domain watermarking schemes achieve better robustness and invisibility. However, in these methods, a constant scaling factor is used to control the watermark embedding strength, which may not applicable for different images. To make a trade-off between robustness and imperceptibility,

Lai [17] proposed a robust watermarking scheme based on SVD and tiny genetic algorithm, where the tiny genetic algorithm was exploited to search for an adaptive scaling factor for watermark embedding. In [18], Mishra et al. firstly analyzed the effect of different scaling factors on the quality of host images and extracted watermarks, and then they proposed an optimized watermarking scheme for grayscale images. An optimal scaling factor is identified by a novel evolutionary algorithm called the firefly algorithm (FA) [19]. Unfortunately, these two methods mentioned above cannot resolve the false positive problem during the watermark extraction process [20,21]. Ansari et al. [22] introduced an integer wavelet transform (IWT) and SVD based watermarking scheme, where the artificial bee colony (ABC) algorithm was applied to determine a best scaling factor. To avoid the false positive problem, an extra signature generated by singular vectors is embedded into the host image along with the watermark.

Though these improved watermarking schemes have achieved great performance, the use of multiple transforms and optimization algorithms increases the complexity of these schemes immensely. In addition, the false positive problem is still a major challenge in SVD domain watermarking schemes. Therefore, a robust image watermarking scheme with less computational cost and without the false positive problem is urgently needed in SVD domain watermarking schemes. In [23], it was pointed out that the essence of transform domain watermarking is to distribute the energy of the embedded signal over all pixels in the spatial domain. Inspired by this, this paper first analyzes the relationship between SVD-based watermarking and the pixel values in the spatial domain, and then proposes a new robust image watermarking scheme using the mathematical characteristics of SVD. Unlike the common SVD domain watermarking schemes, a binary watermark is embedded into the largest singular values of the selected image blocks in the spatial domain. To guarantee the security of this algorithm, the Arnold transform is utilized to encrypt the watermark. Compared with the existing SVD domain watermarking schemes, the proposed method maintains good robustness against signal processing attacks and geometric attacks. Since the watermark embedding process is performed in the spatial domain, the proposed method avoids the false positive problem existing in traditional SVD-based watermarking schemes and reduces the computational complexity.

The remainder of this paper is organized as follows. In Section 2, the basic concepts of SVD and Arnold transform are described briefly. Section 3 analyzes SVD-based watermarking and its impact on the spatial domain. The proposed watermarking scheme is developed in Section 4. Experiments and performance analysis are documented in Section 5. The conclusions and future work are given at the end of this paper.

2. Background

2.1. Singular Value Decomposition (SVD)

Singular value decomposition is a common transform used in numerical analysis. By SVD, a matrix could be decomposed into eigenvectors and eigenvalues [15]. For a matrix $\boldsymbol{A} \in \Re^{m \times m}$, the SVD is defined as:

$$\boldsymbol{A} \Rightarrow \boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}}, \tag{1}$$

where $\boldsymbol{U} \in \Re^{m \times r}$ and $\boldsymbol{V} \in \Re^{m \times r}$ are known as left and right singular vectors, respectively. $\boldsymbol{S} = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_r)$ is a diagonal matrix where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$ are called the singular values of matrix $\boldsymbol{A}$. The singular values have good stability. They can resist the slight disturbances in image processing. In addition, the SVD can be performed on an arbitrary matrix. Owing to these facts, the SVD transform has been widely utilized in robust watermarking schemes for copyright protection.

2.2. Arnold Transform

The Arnold transform, which is also called cat map, is a simple and common encryption algorithm adopted in information hiding. The generalized Arnold transform can be defined as:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{2}$$

where (x_i, y_i) is the original coordinate of image pixel; (x_{i+1}, y_{i+1}) is the scrambled coordinate; and N denotes the width of the image. The Arnold transform has good periodicity, which means that the original image will be reappeared after a certain number of permutations. To guarantee the security of the watermark, the Arnold transform is applied in the proposed scheme, and its iteration time is adopted as a secret key to extract the watermark. It is obvious that without the secret key, the correct watermark cannot be obtained.

3. SVD-Based Watermarking and Its Impact on the Spatial Domain

In this section, we give a brief review of an SVD-based image watermarking and analyze its impact on the pixel values in the spatial domain. In addition, the possibility to achieve SVD-based watermarking in the spatial domain is discussed, which provides a theoretical basis for the design of the proposed watermarking scheme.

3.1. SVD-Based Watermarking

In SVD-based image watermarking [14], the watermark $\boldsymbol{W}$ is embedded into the host image by modifying its singular values. Firstly, the watermark image is decomposed into three parts by SVD:

$$\boldsymbol{W} \Rightarrow \boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}} \boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}}. \tag{3}$$

Then, the host image is decomposed by DWT. The low frequency sub-band (LL) is divided into several non-overlapping blocks. For each block, the SVD is applied. The largest singular value in each block is selected and modulated by the principal component of the watermark image, which can be expressed as:

$$\lambda'_{\max} = \lambda_{\max} + \alpha \boldsymbol{W}_{\boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}}}, \tag{4}$$

where $\lambda_{\max}$ and $\lambda'_{\max}$ represent the original and watermarked largest singular values in the image block, respectively. $\boldsymbol{W}_{\boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}}} = \boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}}$ denotes the principal component of the watermark image, and α is the scaling factor used to control the embedding intensity. In watermark extraction, the principal component of the embedded watermark can be computed by:

$$\boldsymbol{W}_{\boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}}} = \frac{1}{\alpha} (\lambda'_{\max} - \lambda_{\max}). \tag{5}$$

The right singular vector $\boldsymbol{V}_{\mathrm{w}}$ obtained in the watermark embedding process is used as the supplementary information to extract the watermark, which can be expressed as:

$$\boldsymbol{W}_{\boldsymbol{U}_{\mathrm{w}} \boldsymbol{S}_{\mathrm{w}}} \boldsymbol{V}_{\mathrm{w}}^{\mathrm{T}} \Rightarrow \boldsymbol{W}. \tag{6}$$

Due to the good stability of the SVD transform, the SVD-based watermarking scheme and its improvements have achieved great success in copyright protection. However, the false positive problem and the selection of the scaling factor are two major challenges in SVD domain watermarking schemes. In addition, the side information $\boldsymbol{U}_{\mathrm{w}}$ or $\boldsymbol{V}_{\mathrm{w}}$ is needed in watermark extraction, which causes great inconvenience for practical application.

3.2. The Impact of SVD-Based Watermarking on the Pixel Values in the Spatial Domain

From the above analysis, the watermark embedding process of the SVD-based watermarking scheme can be further expressed as:

$$\boldsymbol{A}_{\mathrm{w}} = \boldsymbol{U}(\boldsymbol{S} + \Delta\boldsymbol{S})\boldsymbol{V}^{\mathrm{T}} = \boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}} + \boldsymbol{U}\Delta\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}} = \boldsymbol{A} + \Delta\boldsymbol{A}, \tag{7}$$

where $\boldsymbol{A}$ and $\boldsymbol{A}_{\mathrm{w}}$ denote the image blocks before and after watermark embedding, respectively. $\Delta\boldsymbol{S}$ denotes the watermark information, and $\Delta\boldsymbol{A}$ is the difference matrix between $\boldsymbol{A}$ and $\boldsymbol{A}_{\mathrm{w}}$. From Equation (7), it is noted that the essence of SVD-based watermarking is to distribute the energy of embedded information over all pixels. If we obtain the difference matrix $\Delta\boldsymbol{A}$, SVD-based watermarking could be achieved by directly modifying the pixel values in the spatial domain. Taking a 4×4 image block for example, $\Delta\boldsymbol{A}$ can be calculated by:

$$\begin{aligned}
\Delta\boldsymbol{A} &= \boldsymbol{U}\Delta\boldsymbol{S}\boldsymbol{V}^{\mathrm{T}} = \begin{bmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \boldsymbol{u}_3 & \boldsymbol{u}_4 \end{bmatrix} \Delta\boldsymbol{S} \begin{bmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 & \boldsymbol{v}_4 \end{bmatrix}^{\mathrm{T}} \\
&= \begin{bmatrix} u_1 & u_2 & u_3 & u_4 \\ u_5 & u_6 & u_7 & u_8 \\ u_9 & u_{10} & u_{11} & u_{12} \\ u_{13} & u_{14} & u_{15} & u_{16} \end{bmatrix} \begin{bmatrix} w & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{bmatrix} \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ v_5 & v_6 & v_7 & v_8 \\ v_9 & v_{10} & v_{11} & v_{12} \\ v_{13} & v_{14} & v_{15} & v_{16} \end{bmatrix}^{\mathrm{T}}, \\
&= w \begin{bmatrix} u_1 \\ u_5 \\ u_9 \\ u_{13} \end{bmatrix} \begin{bmatrix} v_1 & v_5 & v_9 & v_{13} \end{bmatrix} = w\boldsymbol{u}_1{\boldsymbol{v}_1}^{\mathrm{T}}
\end{aligned} \tag{8}$$

where $\boldsymbol{u}_i$ and $\boldsymbol{v}_i$ $(i = 1, 2, 3, 4)$ are column vectors in matrices $\boldsymbol{U}$ and $\boldsymbol{V}$; and u_i and v_i $(i = 1, 2, \cdots, 16)$ are their matrix elements, respectively. w denotes the embedded watermark information. It can be seen from Equation (8) that the calculation of $\Delta\boldsymbol{A}$ is equivalent to the solving process of $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$.

In [24], Zhang et al. found that the values in $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ are closely associated with its matrix size, especially when a matrix has similar matrix elements. In this paper, we use this property to develop our proposed scheme. Considering a special case that the matrix $\boldsymbol{A}$ has the same elements, the matrix $\boldsymbol{A}$ can be derived as:

$$\boldsymbol{A} = \begin{bmatrix} a & a & a & a \\ a & a & a & a \\ a & a & a & a \\ a & a & a & a \end{bmatrix} = \begin{bmatrix} \boldsymbol{u}_1 & \boldsymbol{u}_2 & \boldsymbol{u}_3 & \boldsymbol{u}_4 \end{bmatrix} \boldsymbol{S} \begin{bmatrix} \boldsymbol{v}_1 & \boldsymbol{v}_2 & \boldsymbol{v}_3 & \boldsymbol{v}_4 \end{bmatrix}^{\mathrm{T}} = \lambda_1\boldsymbol{u}_1{\boldsymbol{v}_1}^{\mathrm{T}}, \tag{9}$$

where λ_1 is the unique singular value in the diagonal matrix $\boldsymbol{S}$. For an image block with a size of $m \times m$, the value of λ_1 in this particular case is equal to the product between matrix element a and block size m. By Equation (10), the matrix $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ can be obtained.

$$\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}} = \frac{1}{\lambda_1}\boldsymbol{A} = \frac{1}{a \times m} \begin{bmatrix} a & a & a & a \\ a & a & a & a \\ a & a & a & a \\ a & a & a & a \end{bmatrix} = \frac{1}{m} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \tag{10}$$

It is generally known that the local pixel values in each image block have similar pixel values. Based on this characteristic, we promote Zhang et al.'s conclusion to the proposed watermarking scheme. To verify the correctness of this conclusion, several experiments are conducted by utilizing two grayscale images: Lena and Barbara. The images are firstly divided into non-overlapping blocks with a size of $m \times m$. Then, the SVD is performed for each image block, and $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ is calculated. Figure 1 shows the frequency distribution histogram of the elements in $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$, where $m = 2$. From Figure 1a,b, it is

manifested that the matrix elements in $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ are in the normal distribution approximately. Furthermore, most of the elements are gathered in 0.5 (1/2) [24]. To prove the universality of this conclusion, Figure 2 illustrates the frequency distribution histogram of $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ for block sizes 4×4 and 8×8, respectively. It is shown that with the increase of block size, the occurrence frequency of the same elements is decreased. This is because the probability of the similar neighboring pixels in each block becomes much lower than that of the block with a small size. In spite of this, the elements in matrix $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ are still in normal distribution approximately, and most of them are around 0.25 (1/4) and 0.125 (1/8) for the 4×4 block and the 8×8 block, respectively. In other words, most of the values in $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ are closely related to the block size. According to this analysis, the matrix $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ for each image block can be obtained approximately by Equation (10) in the spatial domain. In this way, the difference matrix $\Delta \boldsymbol{A}$ caused by watermark embedding can be approximately calculated based on Equation (8). It is noted that the above analysis provides the possibility to achieve SVD-based watermarking in the spatial domain.

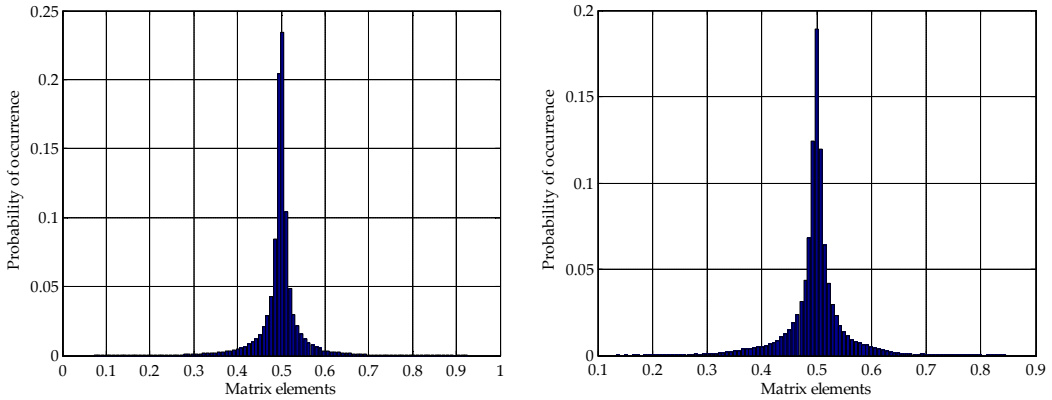

Figure 1. Frequency distribution histogram of the values in $\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$ for block size 2×2: (**a**) Image Lena; (**b**) Image Barbara.

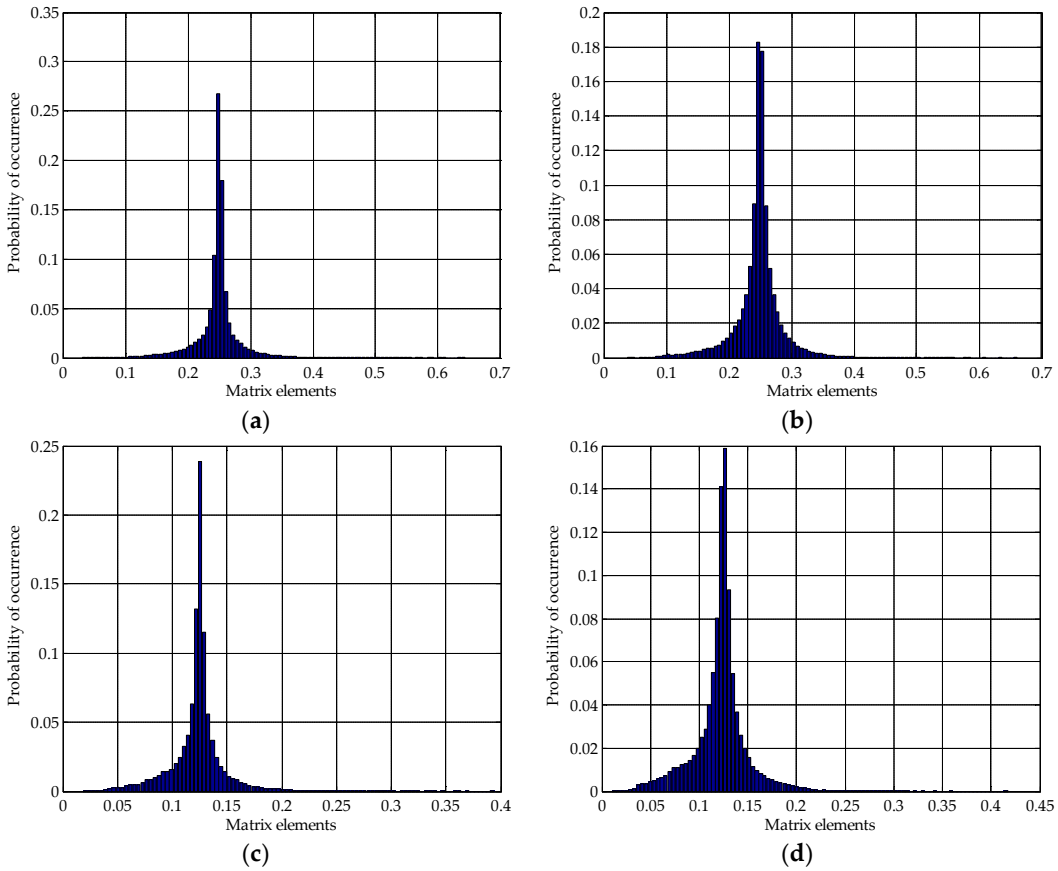

Figure 2. Frequency distribution histogram of the values in $u_1 v_1^{\mathrm{T}}$ for block sizes 4×4 and 8×8: (**a**) Image Lena with block size 4×4; (**b**) Image Barbara with block size 4×4; (**c**) Image Lena with block size 8×8; (**d**) Image Barbara with block size 8×8.

4. The Proposed Scheme

In [23], Su et al. analyzed the relationship between the DCT domain and the spatial domain. Based on this, they proposed a robust DCT-based image watermarking scheme, in which a binary watermark is embedded into the direct current (DC) coefficient of each block in the spatial domain. Based on [23] and the above analysis, a robust SVD-based watermarking scheme in the spatial domain is proposed to protect the copyright of digital images.

4.1. Watermark Embedding

In the proposed method, a binary watermark is embedded into the largest singular values of some image blocks. Figure 3 illustrates the watermark embedding process, and the concrete steps are described as follows.

Step 1. The host image with a size of $M \times M$ is firstly divided into a series of non-overlapping blocks with a size of $m \times m$.

Step 2. The largest singular value $\lambda_{\max}$ in each image block serves as the embedding position to embed the watermark information. Instead of calculating the largest singular value using SVD in SVD-based watermarking [14], the largest singular value is obtained by the 2-norm of a matrix in the spatial domain, which is given by Equation (11). Then, we get a series of singular values $\lambda_{\max}^{i}$ $\{i = 1, 2, \cdots, (M \times M)/(m \times m))\}$.

$$\lambda_{\max} = \|\boldsymbol{A}\|_2. \tag{11}$$

Step 3. It is generally known that the larger the singular value used for watermark embedding is, the smaller the effect of a watermark on the host image will be. To further enhance the watermark imperceptibility, these singular values obtained above are rearranged in descending order, and the larger singular values are selected to embed the watermarking message according to the watermark capacity. In other words, the number of the selected singular values is the same as the number of pixels in the watermark image. In addition, the block indexes of these selected blocks are stored as a key matrix, which will be used for watermark extraction on the receiving end. Therefore, the proposed method is a semi-blind watermarking scheme.

Step 4. To reinforce the safety of the watermark, the binary watermark is encrypted by the Arnold transform with a secret key k.

Step 5. The encrypted watermarking bits are orderly embedded into the largest singular values of the selected blocks by modulating its amplitudes. The embedding rules in [23] are used in this step, which are given as follows.

Let Δ be the quantization step to control the modifying magnitudes T_1 and T_2. The relationship between the watermarking bit w and the modifying magnitudes can be expressed as:

$$\begin{cases} T_1 = 0.5\Delta,\ T_2 = -1.5\Delta,\ w = 1, \\ T_1 = -0.5\Delta,\ T_2 = 1.5\Delta,\ \text{otherwise}. \end{cases} \tag{12}$$

Then, we get the modified singular value $\lambda'_{\max}$ by Equation (13):

$$\begin{aligned} &k_1 = \text{floor}(\text{ceil}(\lambda_{\max}/\Delta)/2), \\ &c_1 = 2k_1\Delta + T_1,\ c_2 = 2k_1\Delta + T_2, \\ &\lambda'_{\max} = \begin{cases} c_2,\ |\lambda_{\max} - c_2| < |\lambda_{\max} - c_1|, \\ c_1,\ \text{otherwise}. \end{cases} \end{aligned} \tag{13}$$

Step 6. To achieve spatial domain watermarking, the difference $\Delta\lambda$ between $\lambda_{\max}$ and $\lambda'_{\max}$ is computed by $\lambda'_{\max} - \lambda_{\max}$. According to Equation (8), we can get the difference matrix $\Delta\boldsymbol{A}$ between the original image block $\boldsymbol{A}$ and its watermarked version $\boldsymbol{A}_{\mathrm{w}}$ using $\Delta\lambda\boldsymbol{u}_1\boldsymbol{v}_1^{\mathrm{T}}$. The watermark embedding process is completed by directly modifying the pixel values using $\Delta\boldsymbol{A}$ in each block, as shown in Equation (7).

Step 7. After image reconstruction, the watermarked image can be obtained.

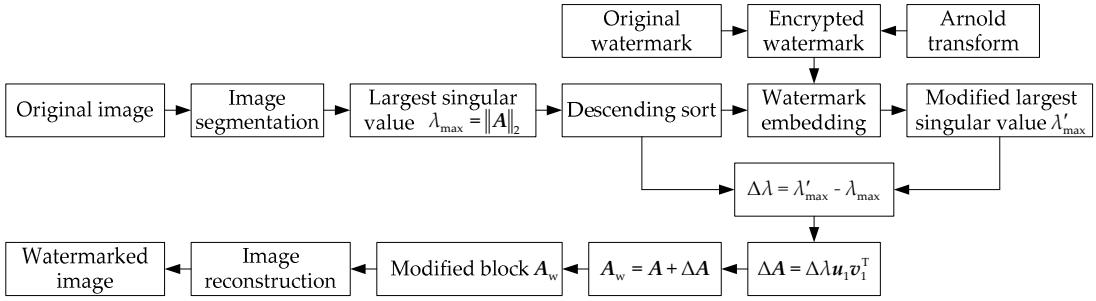

Figure 3. Watermark embedding process.

4.2. Watermark Extraction

Watermark extraction is a relatively simple process. The watermarked image is first divided into non-overlapping blocks with a size of $m \times m$. Then, the blocks embedded with the watermarking bits are determined by the key matrix generated in the watermarking embedding process. The largest singular value $\lambda'_{\max}$ in each block is calculated by the 2-norm operation shown in Equation (11). By the judgment rule given in Equation (14), we get the encrypted binary watermark sequence w from the

watermarked image blocks. After the inverse Arnold transform with the decryption key, the original watermark can be obtained.

$$w = \left[\text{ceil}(\lambda'_{\max}/\Delta)\right] \bmod 2. \tag{14}$$

5. Experimental Results and Performance Analysis

In this section, some experiments are conducted to evaluate the invisibility and robustness of the proposed watermarking scheme. In the experiments, several grayscale images with a size of 512 × 512 are adopted as the host images, and the binary logo of Shandong University with a size of 64 × 64 is selected as the watermark. Figure 4 shows the original host images and the watermark image. To make full use of the conclusion mentioned in Section 3.2, the block size used in this paper is 4 × 4. The secret key k of the Arnold transform is selected as 12.

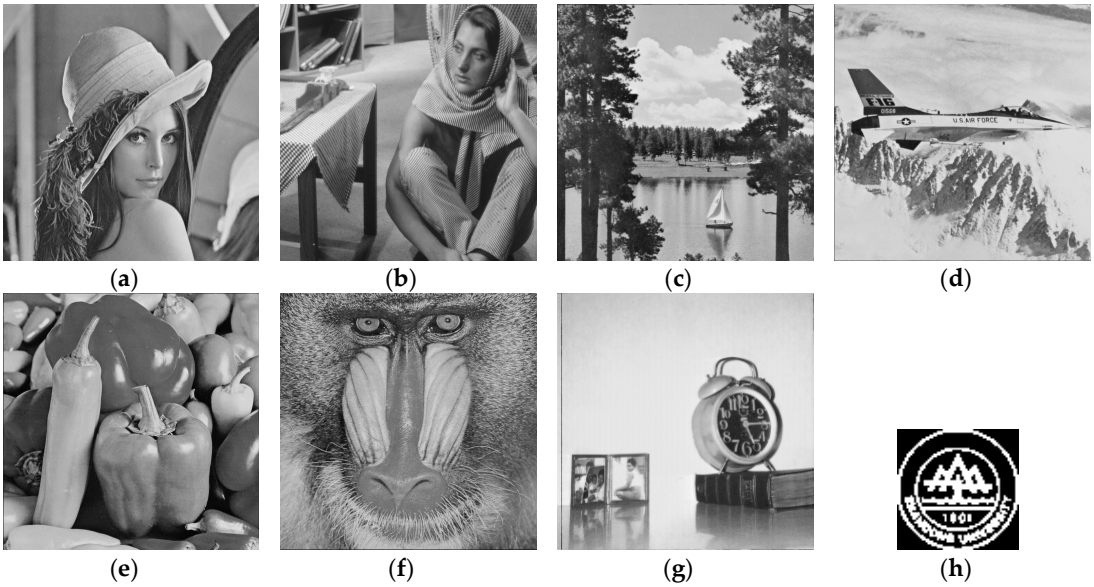

Figure 4. Host images and the original watermark: (**a**) Lena; (**b**) Barbara; (**c**) Boat; (**d**) Airplane; (**e**) Peppers; (**f**) Baboon; (**g**) Clock; (**h**) Original watermark.

As we all know, the imperceptibility and robustness of the watermark is a pair of contradictions in digital watermarking schemes. From the watermark embedding process, it is noted that the larger the quantization step is, the greater the intensity of watermark embedding will be. At the same time, a higher watermark embedding intensity will bring about a greater influence on the quality of the watermarked image. To make a balance between imperceptibility and robustness, we first analyze the effect of different quantization steps on the watermarked images and extracted watermarks. As one of the evaluation indexes of watermark imperceptibility, the structural similarity (SSIM) index [25] is adopted to calculate the similarity between original image and its watermarked version, which is defined as:

$$\text{SSIM} = l(\boldsymbol{I}, \boldsymbol{I}_\text{w}) c(\boldsymbol{I}, \boldsymbol{I}_\text{w}) s(\boldsymbol{I}, \boldsymbol{I}_\text{w}), \tag{15}$$

$$l(\boldsymbol{I}, \boldsymbol{I}_\text{w}) = \frac{2\mu_I \mu_{I_\text{w}} + C_1}{{\mu_I}^2 + {\mu_{I_\text{w}}}^2 + C_1}, c(\boldsymbol{I}, \boldsymbol{I}_\text{w}) = \frac{2\sigma_I \sigma_{I_\text{w}} + C_2}{{\sigma_I}^2 + {\sigma_{I_\text{w}}}^2 + C_2}, s(\boldsymbol{I}, \boldsymbol{I}_\text{w}) = \frac{\sigma_{II_\text{w}} + C_3}{\sigma_I \sigma_{I_\text{w}} + C_3}, \tag{16}$$

where $l(\boldsymbol{I}, \boldsymbol{I}_\text{w})$, $c(\boldsymbol{I}, \boldsymbol{I}_\text{w})$, and $s(\boldsymbol{I}, \boldsymbol{I}_\text{w})$ are three comparison functions for luminance, contrast, and structure, respectively; μ_I and σ_I are the average and variance of the host image $\boldsymbol{I}$; μ_{I_w} and σ_{I_w} are the average and variance of the watermarked image $\boldsymbol{I}_\text{w}$; σ_{II_w} is the covariance between these two images; and C_1, C_2, and C_3 are three parameters used to keep stability. To evaluate the robustness of the proposed method, the normalized correlation coefficient (NCC) is utilized to investigate the

correlation between the original watermark and the extracted watermark. For a watermark image $\boldsymbol{W}$ with a size of $N \times N$, the definition of NCC can be formulated as:

$$\mathrm{NCC} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}[\boldsymbol{W}(i,j) \times \boldsymbol{W}^{*}(i,j)]}{\sum_{i=1}^{N}\sum_{j=1}^{N}[\boldsymbol{W}(i,j)]^{2}}, \tag{17}$$

where $\boldsymbol{W}^{*}$ is the extracted watermark. Both the values of SSIM and NCC range from 0 to 1. In addition, a greater value of SSIM indicates a better watermark invisibility, while a greater value of NCC implies a better robustness. Table 1 lists the SSIM and NCC values of the proposed scheme under different quantization steps. From Table 1, we can notice that the SSIM is decreased with the increase of quantization step. When the quantization step Δ lies between 4 and 16, the quality of the watermarked image does not degrade too much, and the NCC values are equal to 1. Therefore, the quantization step Δ should be selected between 4 and 16. The greater the selected quantization step is, the better the robustness of the proposed scheme will be. However, a greater quantization step will cause more distortion to the visual quality of the host image at the same time. To make a compromise, the quantization step Δ is set to 12 in this paper.

Table 1. Structural similarity (SSIM) index and normalized correlation coefficient (NCC) values of the proposed scheme under different quantization steps.

Quantization Step		**Δ = 1**	**Δ = 2**	**Δ = 4**	**Δ = 8**	**Δ = 16**	**Δ =32**	**Δ = 64**
Lena	SSIM	1	1	0.9991	0.9974	0.9917	0.9707	0.9226
	NCC	0.5014	0.4841	1	1	1	1	1
Barbara	SSIM	1	1	0.9994	0.9983	0.9941	0.9793	0.9422
	NCC	0.4883	0.5021	1	1	1	1	1
Baboon	SSIM	1	1	0.9996	0.9987	0.9957	0.9844	0.9532
	NCC	0.4910	0.5193	1	1	1	1	1

5.1. Imperceptibility Test

To further evaluate watermark imperceptibility, another evaluation metric, known as the peak signal-to-noise ratio (PSNR), is applied in this paper. For an 8-bit image with a size of $M \times M$, the PSNR can be defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{255^{2} \times M \times M}{\sum_{i=1}^{M}\sum_{j=1}^{M}[\boldsymbol{I}(i,j) - \boldsymbol{I}_{\mathrm{w}}(i,j)]^{2}}\ (\mathrm{dB}). \tag{18}$$

In general, a higher PSNR value implies that the watermarked image has better visual quality. It also indirectly demonstrates that the watermarking scheme achieves better watermark invisibility. Figure 5 shows the watermarked images obtained by the proposed scheme. It can be observed that there is almost no distinction between the watermarked images and the original host images subjectively. Table 2 lists the PSNR and SSIM values of the corresponding watermarked images. As shown in Table 2, the PSNR values of the watermarked images are around 49 dB, and the SSIM values are more than 0.99, which further proves the good watermark invisibility of the proposed watermarking scheme.

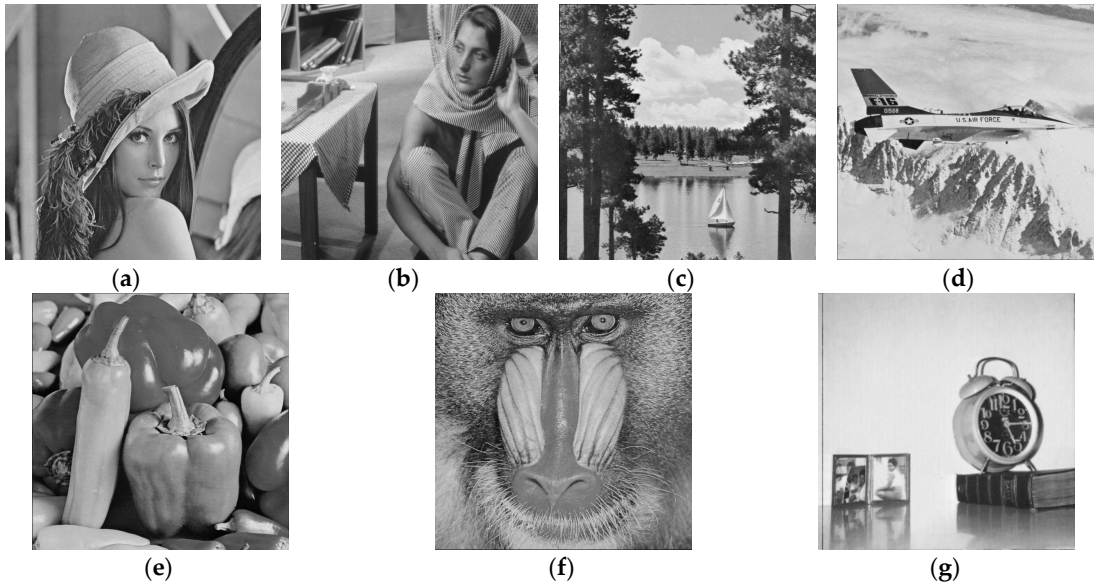

Figure 5. Watermarked images: (**a**) Lena; (**b**) Barbara; (**c**) Boat; (**d**) Airplane; (**e**) Peppers; (**f**) Baboon; (**g**) Clock.

Table 2. Peak signal-to-noise ratio (PSNR) and SSIM values of the watermarked images.

Image	PSNR (dB)	SSIM
Lena	49.07	0.9946
Barbara	48.99	0.9963
Boat	49.09	0.9936
Airplane	49.13	0.9926
Peppers	49.28	0.9951
Baboon	49.06	0.9975
Clock	48.51	0.9890
Average	**49.02**	**0.9941**

5.2. Robustness Test

For the purpose of copyright protection, the watermark should be extracted integrally to prove the ownership of the received image. However, in the process of image transmission and storage, digital images might be destroyed inevitably by various attacks. These attacks can be divided into two broad categories: signal processing attacks and geometric attacks. Signal processing attacks mainly include noise attacks, median filtering, image sharpening, and JPEG compression. They can reduce the energy of watermark information and degrade the visual quality of the extracted watermark. Geometric attacks can destroy the synchronization between the watermark information and the watermarked image. In other words, the watermark information still exists in the image, but their locations have been completely changed. As a result, the watermark might not be found during the watermark extraction process. The most common geometric attacks are image rescaling and image cropping. Therefore, the robustness against these attacks is another key issue in robust watermarking schemes. To test the robustness of the proposed method, these attacks mentioned above are performed on the watermarked images shown in Figure 5. In this paper, we take image Lena as an example to illustrate the robustness of the proposed method. Figure 6 gives the attacked images and the corresponding watermarks extracted from them. From Figure 6, we can see that the extracted watermarks have good visual effect under signal processing attacks and geometric attacks.

Figure 6. Distorted images and the extracted watermarks: (**a**) No attack; (**b**) Salt and pepper noise (0.001); (**c**) Salt and pepper noise (0.005); (**d**) Gaussian noise (0, 0.0001); (**e**) Median filter (3×3); (**f**) Average filter (3×3); (**g**) Image sharpening; (**h**) JPEG (quality factor $Q = 90$); (**i**) JPEG ($Q = 80$); (**j**) JPEG ($Q = 70$); (**k**) Rescaling (2, 0.5); (**l**) Rescaling (0.5, 2); (**m**) Cropping (top 25%); (**n**) Cropping (middle 25%); (**o**) Cropping (right 25%).

5.3. Performance Comparisons

In this subsection, we compare the proposed method with the two SVD domain watermarking schemes in references [8,14]. The method in [8] is a pure SVD-based watermarking scheme, while the method in [14] is a hybrid domain watermarking scheme. Both of these two methods have resolved the false positive problem by embedding the principal component of a watermark into the host image in the SVD domain. To make a better comparison for these three methods, we perform these methods on the images shown in Figure 4 and other test images. Here, we take image Lena and image Barbara as two examples to show the comparison results. Tables 3 and 4 list the NCC values of the extracted watermarks under different attacks. The host images used in Tables 3 and 4 are image Lena and image Barbara, respectively. The PSNR values of the watermarked images are also given in the tables. From the tables, it can be seen that the watermarked images obtained by the proposed scheme have higher

PSNR values compared with the other two methods. In other words, the watermark embedding causes less distortion on the host image. The watermark information can be well hidden in the host image and cannot be discovered by human eyes. After transmission on the Internet, the received images might be destroyed by various attacks. To better present the comparison results, Figures 7 and 8 give the graphic forms of the data in Tables 3 and 4, respectively. From the figures, we can see that the extracted watermarks of the proposed scheme have greater NCC values than the other two methods, except for Gaussian noise and speckle noise. This is because the noise signals of these two kinds of noise are spread all over the pixels, which causes more image distortion than salt and pepper noise. However, for other attacks, our proposed scheme achieves stronger robustness than the other two methods. We would like to note that similar conclusions can be reached when we perform the proposed method on other test images. These conclusions also indirectly indicate that it is feasible to conduct the SVD-based watermarking in the spatial domain.

Table 3. NCC values of the extracted watermarks in image Lena under different attacks.

Attack	Jain et al. [8]	Guo and Prasetyo [14]	The Proposed
PSNR (dB)	21.10	39.26	49.07
No Attack	0.9948	0.9814	1
Salt and Pepper Noise (0.001)	0.9033	0.8442	0.9923
Salt and Pepper Noise (0.005)	0.6383	0.5441	0.9566
Gaussian Noise (0, 0.0001)	0.9598	0.9308	0.9693
Gaussian Noise (0, 0.0005)	0.8426	0.7737	0.7099
Speckle Noise (0.0001)	0.9845	0.9660	0.9944
Speckle Noise (0.0005)	0.9474	0.9098	0.8379
Median Filter (3×3)	0.2306	0.7351	0.9386
Average Filter (3×3)	0.2535	0.5192	0.8641
Image Sharpening	0.9411	0.8545	0.9724
JPEG ($Q = 90$)	0.9591	0.9743	1
JPEG ($Q = 80$)	0.9244	0.9565	0.9986
JPEG ($Q = 70$)	0.8930	0.9176	0.9793
Rescaling (2, 0.5)	0.8276	0.9743	1
Rescaling (0.5, 2)	0.2966	0.8904	0.9538
Cropping (top 25%)	0.3679	0.4581	0.7828
Cropping (middle 25%)	0.3923	0.2812	0.7083
Cropping (right 25%)	0.3351	0.0202	0.7297

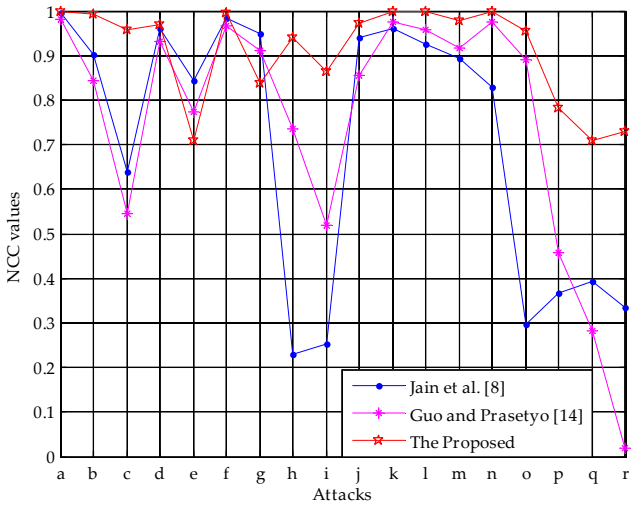

Figure 7. Robustness comparisons for host image Lena: (**a**) No attack; (**b**) Salt and pepper noise (0.001); (**c**) Salt and pepper noise (0.005); (**d**) Gaussian noise (0, 0.0001); (**e**) Gaussian noise (0, 0.0005); (**f**) Speckle noise (0.0001); (**g**) Speckle noise (0.0005); (**h**) Median filter (3×3); (**i**) Average filter (3×3); (**j**) Image sharpening; (**k**) JPEG ($Q = 90$); (**l**) JPEG ($Q = 80$); (**m**) JPEG ($Q = 70$); (**n**) Rescaling (2, 0.5); (**o**) Rescaling (0.5, 2); (**p**) Cropping (top 25%); (**q**) Cropping (middle 25%); (**r**) Cropping (right 25%).

Table 4. NCC values of the extracted watermarks in image Barbara under different attacks.

Attack	Jain et al. [8]	Guo and Prasetyo [14]	The Proposed
PSNR (dB)	21.14	39.26	48.99
No Attack	0.9882	0.9803	1
Salt and Pepper Noise (0.001)	0.8918	0.8290	0.9910
Salt and Pepper Noise (0.005)	0.6257	0.5150	0.9595
Gaussian Noise (0, 0.0001)	0.9524	0.9300	0.9663
Gaussian Noise (0, 0.0005)	0.8347	0.7731	0.6936
Speckle Noise (0.0001)	0.9783	0.9657	0.9939
Speckle Noise (0.0005)	0.9430	0.9118	0.8316
Median Filter (3×3)	0.1548	0.5221	0.7897
Average Filter (3×3)	0.1756	0.4552	0.7469
Image Sharpening	0.8547	0.7921	0.9138
JPEG ($Q = 90$)	0.9425	0.9733	1
JPEG ($Q = 80$)	0.8853	0.9566	0.9952
JPEG ($Q = 70$)	0.8340	0.9168	0.9621
Rescaling (2, 0.5)	0.7447	0.9582	0.9552
Rescaling (0.5, 2)	0.2080	0.8135	0.8497
Cropping (top 25%)	0.2802	0.4705	0.6848
Cropping (middle 25%)	0.3387	0.2955	0.6393
Cropping (right 25%)	0.3987	0.0192	0.8414

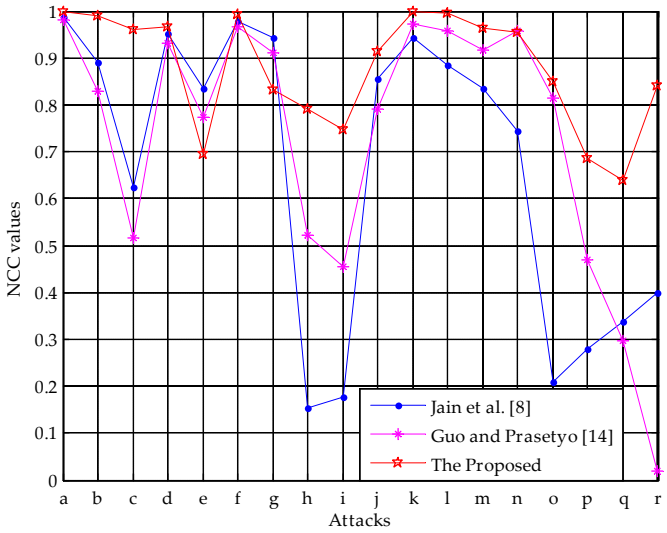

Figure 8. Robustness comparisons for host image Barbara: (**a**) No attack; (**b**) Salt and pepper noise (0.001); (**c**) Salt and pepper noise (0.005); (**d**) Gaussian noise (0, 0.0001); (**e**) Gaussian noise (0, 0.0005); (**f**) Speckle noise (0.0001); (**g**) Speckle noise (0.0005); (**h**) Median filter (3×3); (**i**) Average filter (3×3); (**j**) Image sharpening; (**k**) JPEG ($Q = 90$); (**l**) JPEG ($Q = 80$); (**m**) JPEG ($Q = 70$); (**n**) Rescaling (2, 0.5); (**o**) Rescaling (0.5, 2); (**p**) Cropping (top 25%); (**q**) Cropping (middle 25%); (**r**) Cropping (right 25%).

5.4. Algorithmic Complexity Analysis

To test the algorithmic complexity, the computational time of the proposed spatial domain watermarking scheme is calculated. In addition, we also perform the proposed watermarking scheme in the SVD domain. Unlike the proposed scheme implemented in the spatial domain, it embeds the watermark information into the largest singular values in the SVD domain. Table 5 lists the average computational times of the proposed watermarking scheme and the other two SVD domain watermarking schemes in references [8,14]. To make the conclusions more reliable, we conduct this comparison experiments under the same test conditions. The experiments are performed in the MATLAB R2012a environment and on a 3.10 GHz computer with 6 GB memory. It can be observed

from Table 5 that the proposed spatial domain watermarking scheme has much lower execution times than the proposed scheme implemented in the SVD domain. Compared with the other two watermarking schemes in references [8,14], the computational complexity of the proposed spatial domain watermarking scheme is also reduced. The reason is that the proposed method avoids the forward and inverse SVD transforms used in the SVD domain watermarking schemes.

Table 5. Computational time comparisons between the proposed watermarking scheme and other singular value decomposition (SVD) domain watermarking schemes.

Computational Time (s)	Jain et al. [8]	Guo and Prasetyo [14]	The Proposed	
			SVD Domain	Spatial Domain
Embedding Time	0.4337	0.4721	0.8509	0.3536
Extraction Time	0.2973	0.2805	0.2295	0.1901
Total Time	0.7310	0.7526	1.0804	0.5437

6. Conclusions

Based on the mathematical characteristics of SVD, a robust image watermarking scheme is proposed in this paper. Unlike the common SVD domain watermarking schemes, a binary watermark is inserted into the largest singular values of the selected image blocks in the spatial domain. Before watermark embedding, the watermark image is encrypted by the Arnold transform, which is used to ensure the security of the watermark. To verify the feasibility and performance of the proposed scheme, several experiments are conducted. From the experimental results, it is proved that the proposed watermarking scheme achieves better watermark invisibility and robustness under different attacks. Since the watermark embedding process is performed in the spatial domain, the proposed method avoids the false positive problem existing in traditional SVD-based watermarking and reduces the computational complexity. However, due to the defect of spatial domain watermarking, this method has poor robustness in resisting some other attacks, like image rotation. On the receiving end, some side information is needed to extract the watermark. In other words, the watermark extraction process of the proposed method is not blind. For the future work, we will address these problems and extend the proposed scheme for video copyright protection.

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: Heng Zhang and Chengyou Wang conceived the algorithm and designed the experiments; Heng Zhang performed the experiments; Chengyou Wang and Xiao Zhou analyzed the results; Heng Zhang drafted the manuscript; Xiao Zhou revised the manuscript. All authors have read and approved the final manuscript.

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

References

1. Hai, T.; Li, C.M.; Zain, J.M.; Abdalla, A.N. Robust image watermarking theories and techniques: A review. *J. Appl. Res. Technol.* **2014**, *12*, 122–138.
2. Nyeem, H.; Boles, W.; Boyd, C. Digital image watermarking: Its formal model, fundamental properties and possible attacks. *EURASIP J. Adv. Signal Process.* **2014**, *1*, 1–22. [CrossRef]
3. Su, Q.T.; Wang, G.; Jia, S.L.; Zhang, X.F.; Liu, Q.M.; Liu, X.X. Embedding color image watermark in color image based on two-level DCT. *Signal Image Video Process.* **2015**, *9*, 991–1007. [CrossRef]
4. Keshavarzian, R.; Aghagolzadeh, A. ROI based robust and secure image watermarking using DWT and Arnold map. *AEU Int. J. Electron. Commun.* **2016**, *70*, 278–288. [CrossRef]
5. Liu, R.Z.; Tan, T.N. An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. Multimed.* **2002**, *4*, 121–128.

6. Zhang, X.P.; Li, K. Comments on "An SVD-based watermarking scheme for protecting rightful ownership". *IEEE Trans. Multimed.* **2005**, *7*, 593–594. [CrossRef]
7. Rykaczewski, R. Comments on "An SVD-based watermarking scheme for protecting rightful ownership". *IEEE Trans. Multimed.* **2007**, *9*, 421–423. [CrossRef]
8. Jain, C.; Arora, S.; Panigrahi, P.K. A reliable SVD based watermarking scheme. *Comput. Sci.* **2008**.
9. Lai, C.C.; Tsai, C.C. Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans. Instrum. Meas.* **2010**, *59*, 3060–3063. [CrossRef]
10. Gupta, A.K.; Raval, M.S. A robust and secure watermarking scheme based on singular values replacement. *Sadhana* **2012**, *37*, 425–440. [CrossRef]
11. Fazli, S.; Moeini, M. A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. *Opt. Int. J. Light Electron. Opt.* **2016**, *127*, 964–972. [CrossRef]
12. 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]
13. Guo, J.M.; Prasetyo, H. Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU Int. J. Electron. Commun.* **2014**, *68*, 816–834. [CrossRef]
14. Guo, J.M.; Prasetyo, H. False-positive-free SVD-based image watermarking. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1149–1163. [CrossRef]
15. Ranade, A.; Mahabalarao, S.S.; Kale, S. A variation on SVD based image compression. *Image Vision Comput.* **2007**, *25*, 771–777. [CrossRef]
16. Singh, D.; Singh, S.K. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimed. Tools Appl.* **2017**, *76*, 13001–13024. [CrossRef]
17. Lai, C.C. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digit. Signal Process.* **2011**, *21*, 522–527. [CrossRef]
18. 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]
19. Yang, X.S. Multiobjective firefly algorithm for continuous optimization. *Eng. Comput.* **2013**, *29*, 175–184. [CrossRef]
20. Yavuz, E.; Telatar, Z. Comments on "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm". *Digit. Signal Process.* **2013**, *23*, 1335–1336. [CrossRef]
21. Ali, M.; Ahn, C.W. Comments on "Optimized gray-scale image watermarking using DWT-SVD and firefly algorithm". *Expert Syst. Appl.* **2015**, *42*, 2392–2394. [CrossRef]
22. Ansari, I.A.; Pant, M.; Ahn, C.W. Robust and false positive free watermarking in IWT domain using SVD and ABC. *Eng. Appl. Artif. Intell.* **2016**, *49*, 114–125. [CrossRef]
23. Su, Q.T.; Niu, Y.G.; Wang, Q.J.; Sheng, G.R. A blind color image watermarking based on DC component in the spatial domain. *Opt. Int. J. Light Electron. Opt.* **2013**, *124*, 6255–6260. [CrossRef]
24. Zhang, H.; Wang, C.Y.; Zhou, X. Fragile watermarking for image authentication using the characteristic of SVD. *Algorithms* **2017**, *10*, 27. [CrossRef]
25. Marini, E.; Autrusseau, F.; Callet, P.L.; Campisi, P. Evaluation of standard watermarking techniques. In Proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, San Jose, CA, USA, 26 February 2007; Volume 6505, pp. 1–10.