Optica Applicata, Vol. L, No. 4, 2020
DOI: 10.37190/oa200410

Hybrid watermarking scheme based on singular value decomposition ghost imaging

Jun-Yun WU[1], Wei-Liang HUANG[1], Ru-Hong WEN[2], Li-Hua GONG[3,*]

[1] Department of Computer Science and Technology, Nanchang University,
Nanchang 330031, China

[2] College of Physical Science and Technology, Yichun University,
Yichun 336000, China

[3] Department of Electronic Information Engineering, Nanchang University,
Nanchang 330031, China

[*] Corresponding author: lhgong@ncu.edu.cn

A hybrid watermarking algorithm with an optical watermark image based on singular value decomposition (SVD) ghost imaging is designed. Simultaneously, the blended watermarking algorithm is designed based on 4-level discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD). The 4-level diagonal sub-band image is obtained by performing 4-level two-dimensional wavelet transform on the original image, and the coefficient matrix is produced by applying the discrete cosine transform on the 4-level diagonal sub-band image. Then, three matrices are obtained by performing the singular value decomposition on the coefficient matrix. In addition, the optical watermark image is encrypted by an SVD ghost imaging system. The system could generate a secret key, and unauthorized users could not decrypt and reconstruct the original watermark image without this key. Later the encrypted watermark image is generated into the other three matrices by singular value decomposition. Afterwards, the encrypted watermark is embedded in the host image by mutual operation of different matrices in the algorithm. Simulation results validate the feasibility of the proposed hybrid watermarking scheme.

Keywords: digital watermarking, SVD ghost imaging, discrete wavelet transform, imperceptibility.

1. Introduction

It becomes much easier to distribute, communicate or reproduce multimedia contents with the rapid development of multimedia technology [1]. However, some crucial issues for multimedia, such as illegal copying, distribution, editing and copyright protection have arisen concomitantly [2]. Subsequently, the explosion of digital multimedia products results in rigid demand on security and authenticity of private digital contents [3]. Many optical methods have been devised to hide and encrypt images in the past decades, including the double random-phase encoding (DRPE), ghost imaging (GI), *etc*. [4]. GI, as a novel imaging technology, enables detecting and imaging as separate parts [5]. GI is an imaging method to reconstruct the image of an unknown object by obtaining the field information of the light source, correlating the intensity of two beams of light [6]. In 1995, Pittman *et al*. first proposed the traditional GI method by adopting an object arm and a reference arm [7]. The object arm collects the total light intensity modulated with the object, while the reference arm collects the light intensity directly from the light source [8]. The source is based on an entangled source of two entangled photons, and the imaging process relies on the strength of a second order intensity dependent operation [9]. In 2004, Gatti *et al*. successfully completed an experiment at the first time, employing ghostly imaging with a classic thermal source, and attested that its combination is not a prerequisite [10]. Zhang *et al*. studied pseudo-inverse ghosting imaging (PGI) to calculate the measurement time below the Nyquist limit by calculating the pseudo-inverse of the measurement matrix [11]. Wang *et al*. constructed singular value decomposition ghost imaging (SVDGI), in which a measurement matrix is constructed with monocular value decomposition and the target could be reconstructed by a one-step transposition operation [12]. Even if the measurement result is much smaller than the Nyquist limit in the method, the performances of the GI and the reconstruction time are acceptable [13].

Simultaneously, digital watermarking technology provides a potential solution to information security, which protects the rights and interests of the owners via embedding a certain kind of information into the digital media [14]. Generally, image watermark schemes could be grouped into two categories: watermarking in the spatial domain and watermarking in the transform domain [15]. Spatial domain techniques are the simplest among these techniques, and the watermarks can be embedded directly into pixel intensities of the host signal [16]. However, in transform domain techniques, the watermarks have been usually encrypted by changing the transformed domain coefficients of the host signal [17]. The watermarks embedded in the transform domain are usually more robust than the ones embedded in the spatial domain [18]. The common transform domain methods include fractional Fourier transform (FrFT), discrete cosine transform (DCT) [19], discrete wavelet transform (DWT) [20], singular value decomposition (SVD) [21], *etc*. The performance of transform domain techniques could be further improved with two or more transform domain methods [22]. Ye *et al*. proposed a watermarking scheme based on DWT and SVD, which could resist the geometrical attacks [23]. To handle the false positive detection problem, Gupta and Raval [24] studied a watermarking scheme based on DWT-SVD with incorporating signature-based authentication mechanism. Singh [25] suggested a robust hybrid multiple watermarking technique via fusing DWT, DCT and SVD instead of applying DWT, DCT and SVD individually. In this scheme, the performance of the watermark image has been greatly improved in many aspects [26].

This paper introduces a hybrid watermarking scheme based on singular value decomposition ghost imaging, 4-level DWT, DCT and SVD. Due to the spatial frequency localization characteristics of DWT, the aggregate energy characteristics of DCT and the stability characteristics of SVD, the imperceptibility and the robustness of watermark image could be distinctly improved with these three transforms. Simultaneously, the optical system (SVDGI) could admirably ensure the confidentiality of the watermark image.

The rest of the paper is arranged as follows. In Section 2, a brief theoretical analysis is given. The watermark embedding and extracting scheme are provided in Section 3. The simulation results and the analyses are discussed in Section 4. Finally, a brief conclusion is reached in Section 5.

2. Theoretical background

2.1. Ghost imaging

Ghost imaging is a single-pixel imaging technique based on the correlation between object beam signals and reference beam signals. The object beam and the reference beam are generated by the same light source. The target image is illuminated by the object beam while the light intensity is recorded by a single pixel bucket detector. Simultaneously, the reference beam is directly recorded optically or digitally without interacting with the target object. After a large number of beam pattern illuminations, the original object image could be reconstructed computationally from the recorded intensity sequence with the single pixel detector and corresponding reference illumination patterns. In a similar situation, a ghost imaging system could be designed for information security application, where the recording intensity sequence is the ciphertext and the reference mode is the key.

2.2. Discrete wavelet transform

With excellent space and frequency energy compaction properties, a discrete wavelet transform has become a significant tool in watermarking and image processing. At each layer, DWT decomposes the information of an image into four sub-bands, namely, a lower resolution approximation component (LL) and three spatial direction components corresponding to horizontal component (HL), vertical component (LH) with diagonal

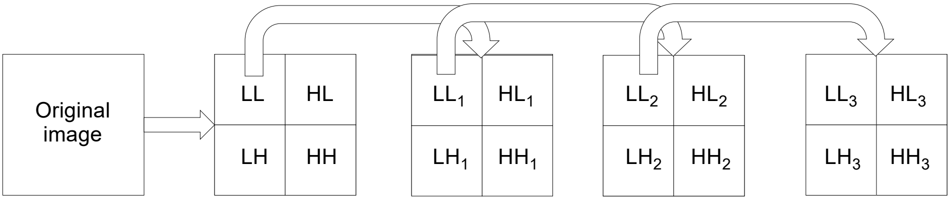

Fig. 1. Four-level wavelet decomposition diagram of image.

component (HH). For better encryption, this paper employs 4-level DWT to achieve signal extraction, as shown in Fig. 1.

2.3. Discrete cosine transform

DCT has distinct properties that most significant information of the image is concentrated on just several low frequency coefficients of the DCT. The 2D DCT transform is defined as

$$F(u, v) = c(u)c(v)\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x, y)\cos\left(\frac{2x+1}{2N}u\pi\right)\cos\left(\frac{2y+1}{2N}v\pi\right) \tag{1}$$

where $x, y, u, v = 0, 1, 2, ..., N-1$, and $c(t) = \begin{cases} 1/\sqrt{2}, & t = 0 \\ 1, & \text{otherwise} \end{cases}$

2.4. Singular value decomposition

SVD is a well-known factorizing method for a real or complex rectangular matrix in numerical analysis. The SVD of **A** is defined as

$$\mathbf{A} = \mathbf{U}\mathbf{S}\mathbf{V}^{\mathrm{T}} \tag{2}$$

where **A** represents an $M \times N$ matrix, **U** and **V** express two orthonormal matrices. **S** is a diagonal matrix composed of the singular values of **A**. The singular values $s_1 \geq s_2 \geq \geq \ldots \geq s_n \geq 0$ are in the descending order along with the main diagonal of matrix **S**.

3. Hybrid watermarking scheme based on SVD ghost imaging

3.1. Implementation of SVDGI

As shown in Fig. 2, the optical experiment setup of SVD ghost imaging system consists of a projector (Panasonic 3LCD) to project the pattern $I_i(x, y)$, a SPD for object $O(x, y)$ (Thorlabs PDA-100A) to collect total reflected light B_i, a data acquisition card to digitize B_i, and a computer to generate $I_i(x, y)$ with restoring objects.

The watermarking image reflection of size $p \times p$ is assumed as $O(x, y)$, and the measurement matrix is a randomly generated matrix $\mathbf{\Phi}$ of size $M \times N$, where $N = p \times p$,

$$\mathbf{\Phi} = \begin{bmatrix} I_1(1, 1) & I_1(2, 2) & \ldots & I_1(p, p) \\ I_2(1, 1) & I_2(2, 2) & \ldots & I_2(p, p) \\ \vdots & \vdots & \ddots & \vdots \\ I_M(1, 1) & I_M(2, 2) & \ldots & I_M(p, p) \end{bmatrix} \tag{3}$$

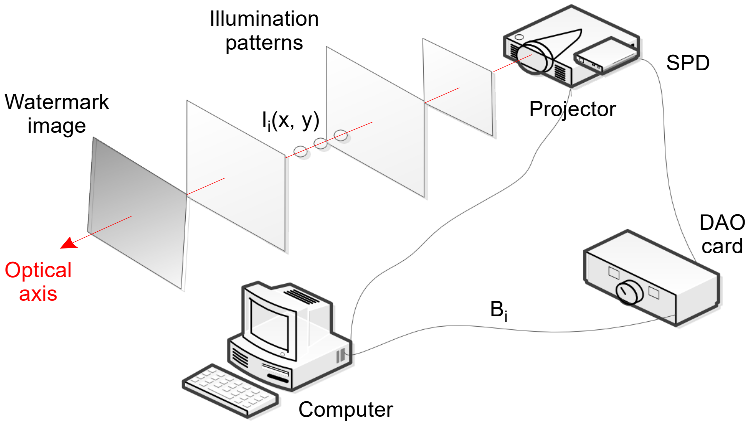

Fig. 2. Optical setup for SVD ghost imaging.

When a $P \times P$ pattern $I_i(x, y)$ is projected onto a line $\mathbf{\Phi}$, the corresponding intensity B_i could be measured. For convenience, the size of $O(x, y)$ is adjusted to a column vector

$$\left[B_1,\ B_2,\ \ldots,\ B_M\right]^{\mathrm{T}} = \mathbf{\Phi}\mathbf{\Phi}\left[O(1, 1),\ O(2, 2),\ \ldots,\ O(p, p)\right]^{\mathrm{T}} \tag{4}$$

where T represents a transposition operation. And

$$\hat{O}(x, y) = \frac{1}{M}\sum_{i=1}^{M}\left(B_i - \langle B\rangle\right) I_i(x, y) \tag{5}$$

where

$$\langle B\rangle = \sum_{i=1}^{M}\frac{B_i}{M} \tag{6}$$

$$B_i = \iint I_i(x, y) O(x, y)\,\mathrm{d}x\,\mathrm{d}y \tag{7}$$

further one has

$$\hat{O}(x, y) = \frac{1}{M}\mathbf{\Phi}^{\mathrm{T}}\mathbf{\Phi}\left[O(1, 1),\ O(2, 2), \ldots,\ O(p, p)\right]^{\mathrm{T}} \tag{8}$$

Even if $M \neq N$, SVDGI could orthogonalize $\mathbf{\Phi}$ by reconstructing the measurement matrix with a modified SVD. After performing SVD on a random $\mathbf{\Phi}$ of size $M \times N$, two orthogonal matrices (**U** and **V**) and a singular value matrix **S**: $\mathbf{\Phi} = \mathbf{USV}^{\mathrm{T}}$ could be obtained. If the non-zero element in **S** turns into 1.0, then the constructed measurement matrix could be written as

$$\mathbf{\Phi}_{\text{SVD}} = \mathbf{U}_{M \times M} |\mathbf{\Sigma}_{M \times M} \mathbf{0}|_{M \times N} \mathbf{V}_{N \times N}^{\text{T}} \tag{9}$$

$$\hat{O}(x, y) = \frac{1}{M} \mathbf{V} \begin{bmatrix} \mathbf{\Sigma}_{M \times M} & 0 \\ 0 & 0 \end{bmatrix}_{N \times N} \mathbf{V}^{\text{T}} O(x, y) \tag{10}$$

where $\mathbf{\Sigma}$ represents the unit matrix. Meanwhile $\mathbf{V}$ still holds the absolute orthogonal character. It shows that the image quality could be significantly improved through replacing $\mathbf{\Phi}$ by $\mathbf{\Phi}_{\text{SVD}}$ at the same number of measurements. Furthermore, the construction time is reduced since only a one-step transposition operation is involved to construct the object, but meanwhile M iterations are required for GI. Prior to encryption, the watermark image is sorted by intensity before being projected onto the object, which could make the encrypted watermark become a grayscale image with little high frequency information after SVDGI sampling, without degrading the image quality.

3.2. Watermark embedding scheme

The image watermark embedding process is described as follows.

Step 1. The host image **I** of size $N \times N$ is partitioned into four sub-bands **LL**, **HL**, **LH** and **HH** with DWT. **LL** is selected as the goal. The low frequency band **LL**, the diagonal detail band $\mathbf{HH}_1$ and the vertical detail band $\mathbf{LH}_2$ are partitioned into sub-bands: $\mathbf{LL}_1$, $\mathbf{HL}_1$, $\mathbf{LH}_1$ and $\mathbf{HH}_1$; $\mathbf{LL}_2$, $\mathbf{HL}_2$, $\mathbf{LH}_2$ and $\mathbf{HH}_2$; $\mathbf{LL}_3$, $\mathbf{HL}_3$, $\mathbf{LH}_3$ and $\mathbf{HH}_3$, successively. $\mathbf{HH}_1$, $\mathbf{LH}_2$ and $\mathbf{HH}_3$ are selected as their sequential steps.

Step 2. Image $\mathbf{J}_1$ could be obtained by applying DCT on the diagonal detail band $\mathbf{HH}_3$,

$$\mathbf{J}_1 = \text{DCT}(\mathbf{HH}_3) \tag{11}$$

Step 3. Image $\mathbf{J}_1$ is decomposed into three matrices **U**, **S** and **V** by SVD,

$$\begin{bmatrix} \mathbf{U} \ \mathbf{S} \ \mathbf{V} \end{bmatrix} = \text{SVD}(\mathbf{J}_1) \tag{12}$$

Step 4. The encrypted watermark image $\mathbf{W}^*$ could be obtained with the SVDGI system executing on the watermark image **W** of size $M \times M$. Meanwhile, the key (modified $\mathbf{\Phi}_{\text{SVD}}$) could be generated with the SVDGI system.

Step 5. Image $\mathbf{W}^*$ is decomposed into three matrices $\mathbf{U}_1$, $\mathbf{S}_1$ and $\mathbf{V}_1$ with SVD,

$$\begin{bmatrix} \mathbf{U}_1 \ \mathbf{S}_1 \ \mathbf{V}_1 \end{bmatrix} = \text{SVD}(\mathbf{W}^*) \tag{13}$$

Step 6. The watermark is embedded in the singular value **S** with a scaling factor k controlling the watermark embedding strength,

$$\mathbf{S}_2 = \mathbf{S} + k \times \mathbf{S}_1 \tag{14}$$

Step 7. According to the matrices **U**, $\mathbf{S}_2$ and **V**, image $\mathbf{J}_2$ could be produced,

$$\mathbf{J}_2 = \mathbf{U}\mathbf{S}_2\mathbf{V}^{\text{T}} \tag{15}$$

Step 8. Image $\mathbf{J}_3$ is obtained by performing the inverse DCT on $\mathbf{J}_2$,

$$\mathbf{J}_3 = \mathrm{IDCT}(\mathbf{J}_2) \tag{16}$$

Step 9. Image $\mathbf{J}_4$ ($\mathbf{J}_5$, $\mathbf{J}_6$ or $\mathbf{I}^*$) could be generated by performing the inverse DWT on $\mathbf{LL}_3$, $\mathbf{HL}_3$, $\mathbf{LH}_3$ and $\mathbf{J}_3$ ($\mathbf{LL}_2$, $\mathbf{HL}_2$, $\mathbf{HH}_2$ and $\mathbf{J}_4$; $\mathbf{LL}_1$, $\mathbf{HL}_1$, $\mathbf{LH}_1$ and $\mathbf{J}_5$; or **HL**, **LH, HH** and $\mathbf{J}_6$).

3.3. Watermark extraction scheme

The watermark extraction process is described as follows.

Step 1. The diagonal matrix **S** after singular value decomposition of the original image is obtained by repeating the watermark embedding process from Step 1 to Step 6. $\mathbf{LL}_4$, $\mathbf{HH}_5$, $\mathbf{LH}_6$, $\mathbf{HH}_7$ are selected as their sequential steps.

Step 2. Image $\mathbf{J}_7$ could be generated by applying DCT on the diagonal detail band $\mathbf{HH}_7$,

$$\mathbf{J}_7 = \mathrm{DCT}(\mathbf{HH}_7) \tag{17}$$

Step 3. Image $\mathbf{J}_7$ is decomposed into three matrices $\mathbf{U}_3$, $\mathbf{S}_3$ and $\mathbf{V}_3$ with SVD,

$$\left[\mathbf{U}_3\ \mathbf{S}_3\ \mathbf{V}_3\right] = \mathrm{SVD}(\mathbf{J}_7) \tag{18}$$

Step 4. The diagonal matrix $\mathbf{S}_4$ of the scrambling watermark image is produced with the scaling factor k and the diagonal matrix **S**,

$$\mathbf{S}_4 = \frac{\mathbf{S}_3 - \mathbf{S}}{k} \tag{19}$$

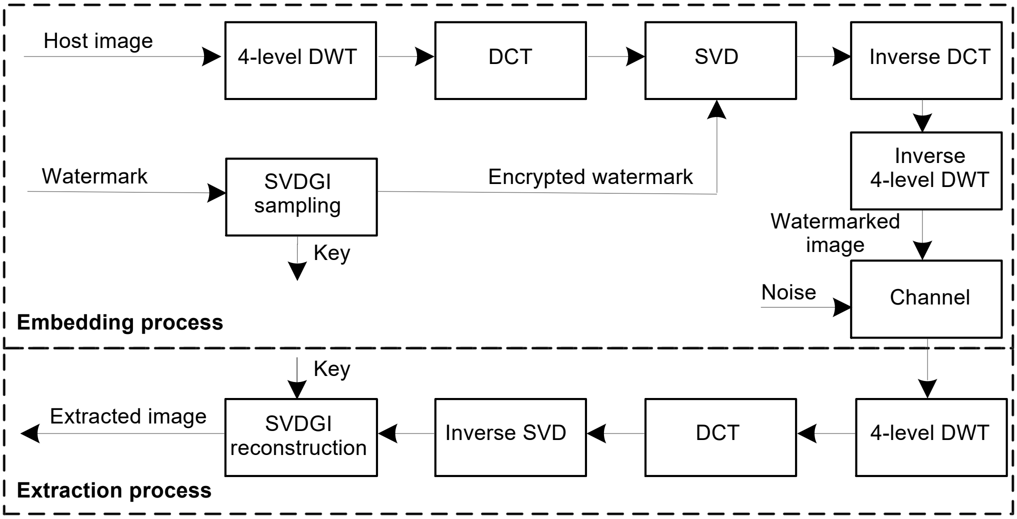

Fig. 3. Proposed image watermarking algorithm.

Step 5. Image $\mathbf{W}^*$ could be obtained with the matrices $\mathbf{U}_1$, $\mathbf{S}_4$ and $\mathbf{V}_1$,

$$\mathbf{W}^* = \mathbf{U}_1 \mathbf{S}_4 \mathbf{V}_1^{\mathrm{T}} \tag{20}$$

Step 6. With $\mathbf{\Phi}_{\mathrm{SVD}}$, the watermark image $\mathbf{W}'$ could be obtained by the SVDGI system. The embedding and the extraction processes of this scheme are shown in Fig. 3.

4. Experiment results and analysis

4.1. Experiment results

The gray images *Lena*, *Barbara*, *Man* and *Baboon* with pixels 512 ×512 serve as the host images, as shown in Fig. 4. And the grayscale image with 32 × 32 pixels shown in Fig. 4**e** is chosen as the watermark. The parameter k in the embedding watermark is set as 0.25. The watermarked images and the extracted watermark images are re-

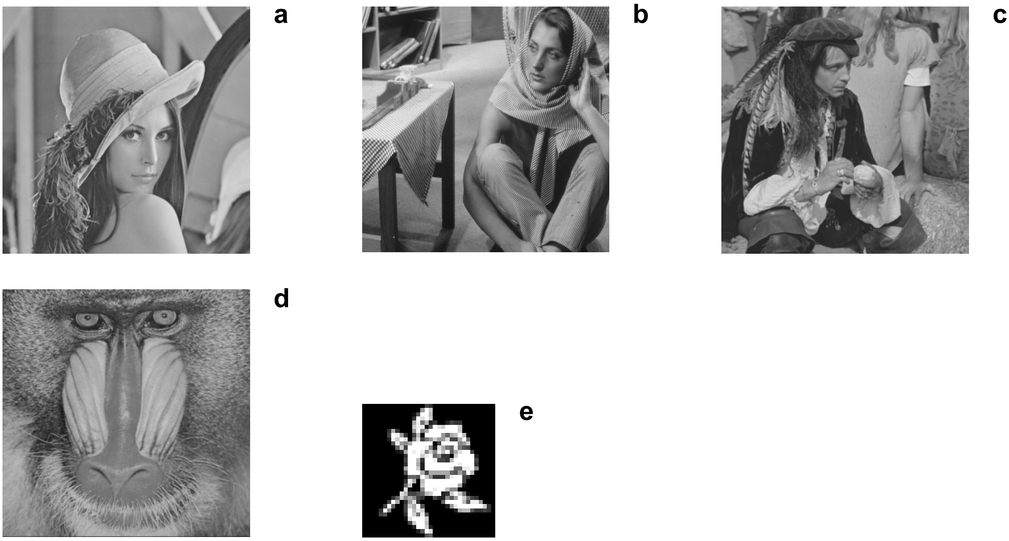

Fig. 4. Test results. Images: *Lena* (**a**), *Barbara* (**b**), *Man* (**c**), and *Baboon* (**d**), and watermark (**e**).

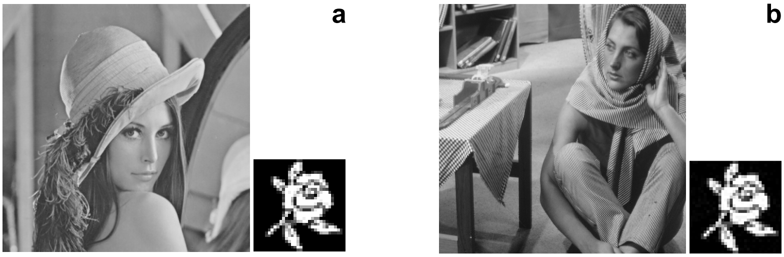

Fig. 5. Watermarked images: *Lena* (**a**), *Barbara* (**b**), *Man* (**c**), and *Baboon* (**d**). Extracted watermarks are also shown.

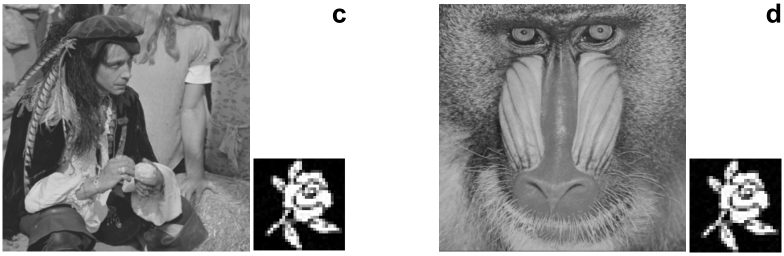

Fig. 5. Continued.

Table 1. PSNR values of the watermarked images.

Cover images	*Lena*	*Barbara*	*Baboon*	*Man*
PSNR [dB]	46.3805	46.6571	45.4523	46.5118

spectively shown in Fig. 5. Apparently, the watermarked images and the host images show no difference. Table 1 presents the PSNR values of the watermarked grayscale images *Lena*, *Barbara*, *Man* and *Baboon*. And the PSNR values of these watermarked images are more than 45 dB. Therefore, the hybrid watermarking scheme based on SVD ghost imaging is feasible.

4.2. Statistical analysis

The robustness of watermarked images with different types of attacks is tested. Normalized correlation (NC) can evaluate the robustness of the algorithm from Ref. [22]. Given an $M \times N$ grayscale image, NC could be defined as

$$\mathrm{NC} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \mathbf{W}(i,j)\,\mathbf{W}^{*}(i,j)\,\mathbf{W}^{2}(i,j)}{\sum_{i=1}^{M} \sum_{j=1}^{N} \mathbf{W}^{2}(i,j)} \tag{21}$$

where $\mathbf{W}$ and $\mathbf{W}^{*}$ are the original watermark and the extracted one, respectively, (i,j) is the coordinate of the current image pixel. SSIM is the structural similarity index, an indicator to measure the similarity of two images [24]. For given two images $\mathbf{X}$ and $\mathbf{Y}$, SSIM is defined as

$$\mathrm{SSIM}(\mathbf{X},\mathbf{Y}) = \frac{(2\mu_{\mathrm{X}}\mu_{\mathrm{Y}} + c_1)(2\sigma_{\mathrm{XY}} + c_2)}{(\mu_{\mathrm{X}}^2 + \mu_{\mathrm{Y}}^2 + c_1)(\sigma_{\mathrm{X}}^2 + \sigma_{\mathrm{Y}}^2 + c_2)} \tag{22}$$

where μ_{X} and μ_{Y} are the mean values of $\mathbf{X}$ and $\mathbf{Y}$, respectively; σ_{X} and σ_{Y} are the standard deviations of $\mathbf{X}$ and $\mathbf{Y}$, respectively, σ_{XY} is the cross-correlation, $c_1 = (0.01L)^2$, $c_2 = (0.03L)^2$, L is the gray level.

To test the robustness of the proposed hybrid watermarking scheme based on SVD ghost imaging, various attacks are performed on the watermarked images *Lena*

Table 2. NC and SSIM values of *Lena* and *Barbara* after various attacks.

Attacks	*Lena*		*Barbara*	
	NC	SSIM	NC	SSIM
No attack	0.9956	0.9979	0.9947	0.9992
Salt-and-pepper noise (0.1)	0.9512	0.9302	0.9662	0.9461
Salt-and-pepper noise (0.3)	0.9287	0.8816	0.9636	0.9056
salt-and-pepper noise (0.5)	0.9141	0.8793	0.9406	0.8969
JPEG compression (90%)	0.9793	0.9943	0.9987	0.9973
JPEG compression (60%)	0.8396	0.9411	0.9053	0.9843
JPEG compression (30%)	0.6651	0.8054	0.7868	0.9365
Irregular cutting	0.9534	0.9757	0.8532	0.9739
1/4 cutting	0.9155	0.9071	0.7316	0.8754
1/2 cutting	0.8416	0.7165	0.5533	0.4213
Gaussian noise (0.1)	0.9241	0.9067	0.9664	0.9172
Gaussian noise (0.3)	0.9279	0.8915	0.9483	0.9056
Gaussian noise (0.5)	0.9188	0.8808	0.9395	0.8936
Image brightening	0.6169	0.7982	0.4773	0.5872
Image darkening	0.8017	0.9526	0.7401	0.9123
Contrast variation enhance	0.8698	0.8848	0.8713	0.8731
Contrast variation weaken	0.6002	0.7815	0.4773	0.5872

and *Barbara*, and the results are shown in Table 2. Under different intensities of the salt-and-pepper noise, the NC values and the SSIM values are acceptable. Therefore, the proposed hybrid watermarking scheme based on SVD ghost imaging is robust against the salt-and-pepper noise attacks. Simultaneously, the NC values are more than 0.6 while the SSIM values are greater than 0.8, which indicates that the extracted watermark image after the JPEG compression attack has a high structural similarity and is significantly correlated with the original watermark image. Besides, the NC values and the SSIM ones are consistent with the requirements of robustness when the watermarked images face other noise attacks, such as Gaussian noise attack, contrast variation attack, *etc.*

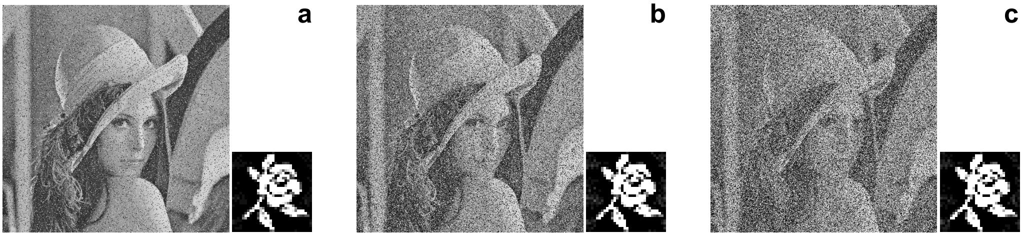

Fig. 6. Results of salt-and-pepper noise attack. Watermarked *Lena* correspond to noise intensities 0.1 (**a**), 0.3 (**b**), and 0.5 (**c**). Extracted watermarks are also shown.

For simplicity, only image *Lena* from these images in experiment is displayed. The results of the salt-and-pepper noise attack on image *Lena* are displayed in Fig. 6. Apparently, the watermark image can still be extracted, since DCT in the watermark scheme could suppress the salt-and-pepper noise.

Figure 7 exhibits the results of the JPEG compression attack on the watermarked image *Lena*. These results indicate that the extracted watermark image after the JPEG compression attack is significantly correlated with the original watermarking image and possesses a high structural similarity. Under high compression conditions, the hybrid watermark scheme could still extract the watermark images. Thus, the proposed hybrid watermark scheme could resist the JPEG compression attack to some degree.

Figure 8 gives the results of the watermarked images and the corresponding extracted watermarks under irregular cutting or different degrees of cutting and Gaussian noise attacks. Under different cutting attacks and Gaussian noise attacks, the watermark infor-

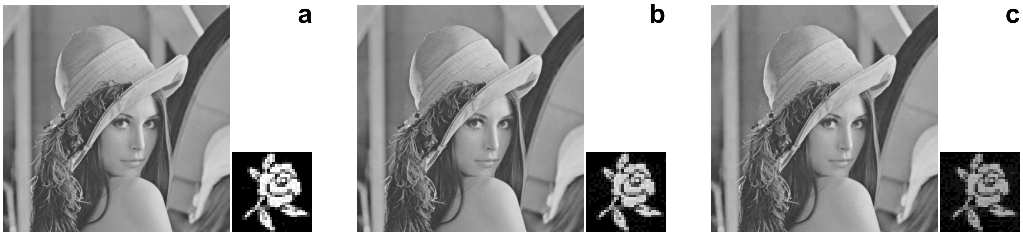

Fig. 7. Results of the JPEG compression attack. Watermarked image *Lena* correspond to compression factors 90% (**a**), 60% (**b**), and 30% (**c**). Extracted watermarks are also shown.

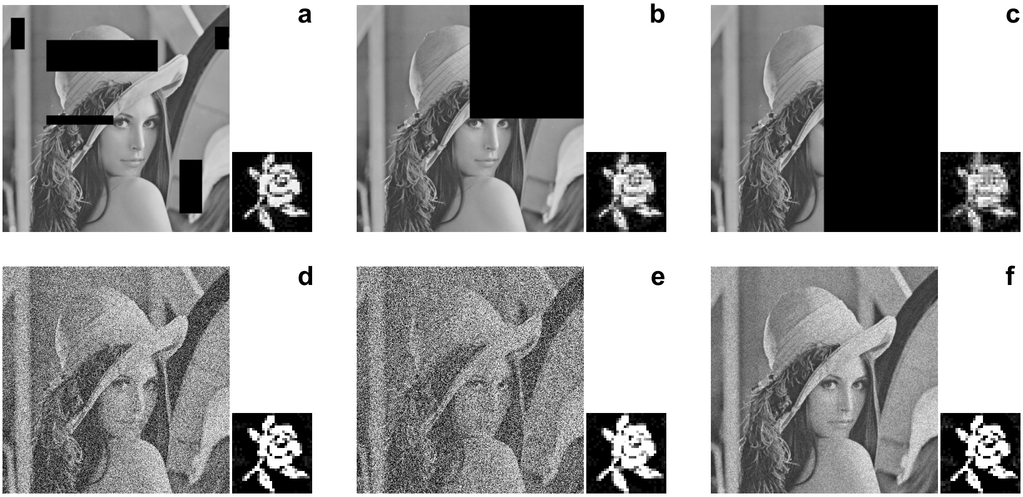

Fig. 8. Results of the cutting attack and Gaussian noise attack. Watermarked image *Lena*: irregular cutting (**a**), 1/4 cutting (**b**), 1/2 cutting (**c**), with variances 0.1 (**d**), 0.3 (**e**), and 0.5 (**f**). Extracted watermarks are also shown.

mation could still be extracted from the watermarks, although the quality of the extracted watermarks becomes worse as the noise intensity increases. Therefore, the proposed hybrid watermark scheme based on singular value decomposition ghost imaging could resist the cutting attack and Gaussian noise attack.

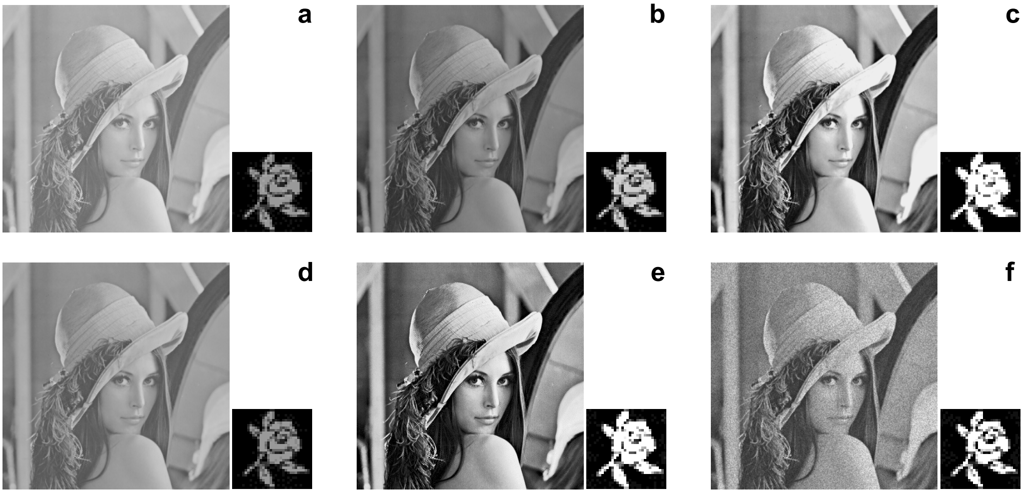

Fig. 9. Results of different attacks. Watermarked image *Lena*: image brightness (**a**), image darkening (**b**), contrast enhance (**c**), contrast weaken (**d**), histogram equalization (**e**), multiplicative noise (**f**). Extracted watermarks are also shown.

Table 3. Comparisons of normalized correlation coefficient with existing schemes.

Attacks	Existing schemes			Proposed scheme
	Ref. [12]	Ref. [24]	Ref. [26]	
Encryption method	SVDGI, LWT	DWT, SVD	DWT, DCT, SVD	SVDGI, 4-DWT, DCT, SVD
No attack	0.9889	0.9979	0.9983	0.9980
Salt-and-pepper noise (0.1)	0.9130	0.9302	0.9443	0.9512
Salt-and-pepper noise (0.5)	0.6601	0.8793	0.9101	0.9141
JPEG compression (90%)	0.9105	0.9426	0.9837	0.9943
JPEG compression (30%)	0.6241	0.6203	0.7968	0.8054
Irregular cutting	0.9189	0.9538	0.9696	0.9757
1/4 cutting	0.8125	0.9071	0.9102	0.9155
1/2 cutting	0.7483	0.7165	0.8042	0.8416
Gaussian noise (0.1)	0.9170	0.9067	0.9196	0.9241
Gaussian noise (0.5)	0.8781	0.8808	0.9123	0.9188
Image brightening	0.5995	0.6983	0.8753	0.7982
Image darkening	0.7948	0.8556	0.9435	0.9526
Contrast variation enhance	0.8672	0.8993	0.8796	0.8848
Contrast variation weaken	0.6162	0.8015	0.8049	0.7815

Figure 9 shows the results of different attacks on the watermarked image *Lena*, including brightness transform attack, contrast variation attack, histogram equalization and multiplicative noise attack. The watermark images could be clearly identified, hence the proposed watermark scheme based on SVD ghost imaging could stand up to these attacks.

4.3. Comparison

To further reflect the advantages of the proposed hybrid watermark scheme based on SVD ghost imaging, the comparison results with several previous methods are compiled in Table 3. SVDGI could achieve encryption function [12]. By embedding watermark into an approximation sub-band, the ability to resist JPEG compression is high [24]. However, this method could not achieve preferable results under other noise attacks with DWT. And the combination of DWT, DCT and SVD apparently improved the robustness of the algorithm in Ref. [26]. Furthermore, 4-DWT and SVDGI in the proposed watermarking scheme could achieve acceptable results.

5. Conclusion

A hybrid optical watermarking scheme based on singular value decomposition ghost imaging, 4-level DWT, DCT and SVD is proposed. Considering the requirements of the human visual system at the masking characteristics of image brightness, texture and frequency, the host image is processed by 4-level DWT and DCT, which greatly enhances the imperceptibility and the robustness of the watermarked image. And in the watermark embedding process, the SVD with good stability characteristic further enhances the robustness of the watermarked image. Simultaneously, the optical SVD ghost imaging system is designed to encrypt the watermark image, which could greatly improve the confidentiality of the watermark image before the embedding process. Ultimately the encrypted watermark is embedded in the host image by mutual operation of different matrices. Simulation results demonstrate that the hybrid digital watermarking scheme could resist different digital signal processing attacks, such as JPEG compression attack, salt-and-pepper noise attack, Gaussian noise attack, filtering attack, brightness change attack, geometric attack, cutting attack, *etc*.

Acknowledgements – This work is supported by the National Natural Science Foundation of China (Grant No. 61861029), and the Cultivation Plan of Applied Research of Jiangxi Province (Grant No. 20181BBE58022).

References

[1] Khan A., Siddiqa A., Munib S., Munib S., *A recent survey of reversible watermarking techniques*, Information Sciences **279**, 2014, pp. 251–272, DOI: 10.1016/j.ins.2014.03.118.

[2] Lang J., Zhang Z.G., *Blind digital watermarking method in the fractional Fourier transform domain*, Optics and Lasers in Engineering **53**, 2014, pp. 112–121, DOI: 10.1016/j.optlaseng.2013.08.021.

[3] Singh H., *Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain*, Optica Applicata **47**(4), 2017, pp. 557–578, DOI: 10.5277/oa170406.

[4] Leenhardt R., Vasseur P., Li C., Saurin J.C., Rahmi G., Cholet F., Becq A., Marteau P., Histace A., Dray X., *A neural network algorithm for detection of GI angiectasia during small-bowel capsule endoscopy*, Gastrointestinal Endoscopy **89**(1), 2019, pp. 189–194, DOI: 10.1016/j.gie.2018.06.036.

[5] Chen W., *Optical cryptosystem based on single-pixel encoding using the modified Gerchberg–Saxton algorithm with a cascaded structure*, Journal of the Optical Society of America A **33**(12), 2016, pp. 2305 –2311, DOI: 10.1364/JOSAA.33.002305.

[6] Wen J.Y., Gong N.S., Chen Y., *Blind image watermarking algorithm based on compressed sensing*, Journal of Scientific Computing **43**, 2016, pp. 377–382 (in Chinese).

[7] Pittman T.B., Shih Y.H., Strekalov D.V., Sergienko A.V., *Optical imaging by means of two-photon quantum entanglement*, Physical Review A **52**(5), 1995, pp. R3429–R3432, DOI: 10.1103/PhysRevA.52.R3429.

[8] Fan D.S., Meng X.F., Wang Y.R., Yang X.L., Peng X., He W.Q., Dong G.Y., Chen H.Y., *Optical identity authentication scheme based on elliptic curve digital signature algorithm and phase retrieval algorithm*, Applied Optics **52**(23), 2013, pp. 5645–5652, DOI: 10.1364/AO.52.005645.

[9] Hsu L.Y., Hu H.T., *Robust blind image watermarking using crisscross inter-block prediction in the DCT domain*, Journal of Visual Communication and Image Representation **46**, 2017, pp. 33–47, DOI: 10.1016/j.jvcir.2017.03.009.

[10] Gatti A., Brambilla E., Bache M., Lugiato L.A., *Ghost imaging with thermal light: comparing entanglement and classical correlation*, Physical Review Letters **93**(9), 2004, article 093602, DOI: 10.1103/PhysRevLett.93.093602.

[11] Zhang C., Guo S.X., Cao J.S., Guan J., Gao F.L., *Object reconstitution using pseudo-inverse for ghost imaging*, Optics Express **22**(24), 2014, pp. 30063–30073, DOI: 10.1364/OE.22.030063.

[12] Wang S.Q., Meng X.F., Yin Y.K., Wang Y.R., Yang X.L., Zhang X., Peng X., He W.Q., Dong G.Y., Chen H.Y., *Optical image watermarking based on singular value decomposition ghost imaging and lifting wavelet transform*, Optics and Lasers in Engineering **114**, 2019, pp. 76–82, DOI: 10.1016/j.optlaseng.2018.10.014.

[13] Zhang X., Meng X.F., Yang X.L., Wang Y.R., Yin Y.K., Li X.Y., Peng X., He W.Q., Dong G.Y., Chen H.Y., *Singular value decomposition ghost imaging*, Optics Express **26**(10), 2018, pp. 12948 –12958, DOI: 10.1364/OE.26.012948.

[14] Zhou N.R., Luo A.W., Zou W.P., *Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm*, Multimedia Tools and Applications **78**(2), 2019, pp. 2507 –2523, DOI: 10.1007/s11042-018-6322-9.

[15] Lu W.H., Chen Z.L., Li L., Cao X.C., Wei J.G., Xiong N.X., Li J., Dang J.W., *Watermarking based on compressive sensing for digital speech detection and recovery*, Sensors **18**(7), 2018, article 2390, DOI: 10.3390/s18072390.

[16] Loganathan A., Kaliyaperumal G., *An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system*, Expert Systems With Applications **63**, 2016, pp. 412–434, DOI: 10.1016/j.eswa.2016.05.019.

[17] Al-Otum H.M., Samara N.A., *A robust blind color image watermarking based on wavelet-tree bit host difference selection*, Signal Processing **90**(8), 2010, pp. 2498–2512, DOI: 10.1016/j.sigpro.2010.02.017.

[18] Bassel A., Nordin M.J., *Digital image watermark authentication using DWT-DCT*, Journal of Engineering and Applied Sciences **11**(14), 2016, pp. 3227–3232, DOI: 10.36478/jeasci.2016.3227.3232.

[19] Singh R.K., Shaw D.K., Sahoo J., *A secure and robust block based DWT-SVD image watermarking approach*, Journal of Information and Optimization Sciences **38**(6), 2017, pp. 911–925, DOI: 10.1080/02522667.2017.1372137.

[20] Alves D.K., Ribeiro R.L.A., Costa F.B., Rocha T.O.A., *Real-time wavelet-based grid impedance estimation method*, IEEE Transactions on Industrial Electronics **66**(10), 2019, pp. 8263–8265, DOI: 10.1109/TIE.2018.2870407.

[21] Zhou X., Zhang H., Wang C.Y., *A robust image watermarking technique based on DWT, APDCBT and SVD*, Symmetry **10**(3), 2018, article 77, DOI: 10.3390/sym10030077.

[22] Zhou N.R., Hou W.M.X., Wen R.H., Zou W.P., *Imperceptible digital watermarking scheme in multiple transform domains*, Multimedia Tools and Applications **77**(23), 2018, pp. 30251–30267, DOI: 10.1007/s11042-018-6128-9.

[23] Ye X., Chen X., Deng M., Wang Y.L., *A SIFT-based DWT-SVD blind watermark method against geometrical attacks*, [In] *2014 7th International Congress on Image and Signal Processing*, 2015, pp. 323–329, DOI: 10.1109/CISP.2014.7003800.

[24] Gupta A.K., Raval M.S., *A robust and secure watermarking scheme based on singular values replacement*, Sadhana **37**(4), 2012, pp. 425–440, DOI: 10.1007/s12046-012-0089-x.

[25] Singh A.K., *Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images*, Multimedia Tools and Applications **76**(6), 2017, pp. 8881–8900, DOI: 10.1007/s11042-016-3514-z.

[26] Singh D., Singh S.K., *DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection*, Multimedia Tools and Applications **76**(11), 2017, pp. 13001–13024, DOI: 10.1007/s11042-016-3706-6.

Received October 2, 2019
in revised form March 2020