

基于 DD-PCA 的可靠性水印改进算法

王欢欢 周粟婷

(上海大学 上海电影学院 上海 200072)

摘 要: 针对基于奇异值分解(SVD)算法常有的高虚警问题,提出了基于双重分解主成分分析 DD-PCA 的可靠性图像水印改进技术。算法对水印图像采用 SVD 方法进行主成分提取,然后将提取的水印图像主成分嵌入到载体图像的 SVD 变换的奇异值中,创新性地对嵌入主成分后的奇异值进行二次奇异值分解,进行 ISVD (inverse-SVD) 变换即可得到嵌入水印的图像。通过该方法使得提出的算法具有较好的水印不可见性,通过进行加噪、压缩、模糊、几何变形攻击,验证了算法具有较好的鲁棒性。

关键词: 奇异值分解;双重分解主成分分析;虚警问题

中图分类号: TP309; TN919.8 **文献标识码:** A **国家标准学科分类代码:** 520.6040

DD-PCA based improved watermarking with reliability

Wang Huanhuan Zhou Jiting

(Shanghai Film Academy, Shanghai University, Shanghai 200072, China)

Abstract: To Solving the high false problem of SVD (singular value decomposition) based algorithm, a DD-PCA (double-decomposition principal component analysis) based improved image watermarking algorithm with reliability is proposed in this paper. The principal component of the watermark is extracted with SVD and embedded into the singular values of the host image. Then the second SVD is used creatively. After ISVD, the watermarked image is obtained. Experimental results show that the algorithm proposed is well imperceptible and robust to noising, compression, blurring and geometric attacks.

Keywords: singular value decomposition; DD-principal component analysis; false positiv

0 引 言

随着计算机发展,数字媒体如图像、视频等的复制、存取和传播变得非常方便,但同时数字媒体的安全和版权问题也变得尤为重要。数字水印^[1-3]技术作为信息隐藏技术研究领域的重要分支,在数字产品版权保护和数据安全维护方面发挥重要作用。2002 年,基于奇异值分解(singular value decomposition, SVD)的数字水印属于变换域的一种,被 Liu 提出来,后成为众多学者研究数字水印的方向^[4-5],也是目前较为主流的方法之一。Loukhaoukha^[6]深入分析了 Liu 的算法,指出基于 SVD 的水印算法有虚警(false positive)问题。即使用不同于嵌入的水印图像的另一图像进行提取,也可以提取出水印图像,造成版权模糊情况(ambiguous situation),即无法确认版权归属。攻击者可以很容易在不知道原始嵌入的水印的情况下,找到一个参考水印图像,证明是图像版权所有者。假设对两幅图像 A 和 B 进行 SVD 计算 $A \Rightarrow U_A \Sigma_A V_A^T$ $B \Rightarrow U_B \Sigma_B V_B^T$,再交换两幅

图像的奇异值得到 $U_A \Sigma_B V_A^T \approx A$ $U_B \Sigma_A V_B^T \approx B$,这是产生虚警问题的原因,是大多数基于 SVD 分解的水印算法^[7-9]用于版权保护亟待解决的问题。

一部分人针对基于 SVD 的水印算法中产生的虚警问题利用主成分分析(principal component analysis, PCA)方法解决,提出了可靠的 SVD 算法。Jain 等人根据 SVD 分解的两个酉矩阵 U 和 V^T 保留了水印图像重要信息的原理,将水印的主成分嵌入到图像的奇异值中,而不是传统的仅仅嵌入水印的奇异值的方法,这种尝试有效解决了在文献[7-9]中出现的问题,但是产生新问题:水印嵌入强度因子对不可见性和鲁棒性产生很大影响,水印嵌入强度越小,不可见性越高,但鲁棒性减弱,反之,亦然。在 Jain 等人算法的基础上,一些人进行了深入的和进一步研究,Run 等人^[10]也进行改进,在 DCT 与 DWT 域中进行试验,提取水印图像的 PC 矩阵,采用粒子群优化算法(particle swarm optimization, PSO)在一定程度上选择较合适的嵌入强度因子嵌入到载体图像的奇异值中,最后进行奇异值逆变换得

到嵌入水印图像,嵌入过程结合 DCT 和 DWT 特点。结果表明该算法具有较好的不可见性和鲁棒性,并有效地解决了虚警问题和版权模糊情况,但算法过于复杂,本文提出的 PSO 算法虽然能一定程度地使得嵌入强度因子具有适应性,但并不能从根本上解决嵌入因子的选择问题。嵌入强度因子的选择一直是数字水印中的研究难点,目前现有方法中,尚未有公认的最好的解决办法,大多数算法采取反复实验 (trial-and-error) 的方法来确定嵌入强度因子。Loukhaoukha 等人^[11]对待嵌入载体图像利用 SVD 方法提取 PC 矩阵,之后在提取的载体图像 PC 矩阵中嵌入水印。此方法提取时无需原始水印图像,不存在虚警问题,但水印不可见性和鲁棒性受嵌入强度因子影响较大。

综上,现有的基于 SVD 的可靠性算法存在无法平衡不可见性和鲁棒性、算法复杂度高等问题,本文对此进行改进,在进行主成分嵌入之后进行二次奇异值分解,并精炼算法,实验结果证明算法具有较好的水不可见性和鲁棒性,可支持较大范围的嵌入强度因子,在一定程度上对二者进行了平衡。

1 基于 SVD 的图像水印算法

1.1 奇异值分解

SVD 定义为假设 $\mathbf{A}$ 为大小为 $N \times M$ 的图像,则其奇异值分解为:

$$\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T \quad (1)$$

式中: T 为转置符号。 $\mathbf{U}$ 和 $\mathbf{V}$ 为奇异向量,称为酉矩阵,大小分别为 $N \times N$ 和 $M \times M$,分别满足 $\mathbf{U}\mathbf{U}^T = \mathbf{U}^T\mathbf{U} = \mathbf{I}_N$ $\mathbf{V}\mathbf{V}^T = \mathbf{V}^T\mathbf{V} = \mathbf{I}_M$, $\mathbf{I}_N$ 和 $\mathbf{I}_M$ 是单位阵。

$\mathbf{\Sigma}$ 为大小 $N \times M$ 的奇异值矩阵,非对角元素为 0,对角线上元素为奇异值,如下:

$$\mathbf{\Sigma} = \begin{bmatrix} \mathbf{\Sigma}_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \quad \mathbf{\Sigma}_r = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_r) \quad (2)$$

式中: $\mathbf{\Sigma}_r$ 为方阵,对角线上的 $\sigma_1, \sigma_2, \dots, \sigma_r$ 为 $\mathbf{A}$ 的奇异值。

图像奇异值分解有很多显著特性如下:

1) 适用于非方阵的图像,大多数的算法是不能直接处理非方阵的图像;

2) 图像奇异值的稳定性好,对图像施加小的扰动时,其奇异值不会有大的变化;

3) 奇异值代表图像内蕴的能量信息, $\mathbf{U}$ 和 $\mathbf{V}^T$ 体现图像的几何、纹理等视觉特性;

4) 当图像几何失真(转置、镜像、放大、平移、旋转)时,奇异值仍具有不变性;

5) 可使用前 r 个大的奇异值来近似图像矩阵 $\mathbf{A}$, 如下:

$$\mathbf{A}_{N \times M} \approx \mathbf{U}_{N \times r} \mathbf{\Sigma}_{r \times r} \mathbf{V}_{M \times r}^T \quad (3)$$

由于其显著特点使得其广泛用于数字水印中,对奇异值进行小范围的改变来嵌入水印,不会引起视觉上的变化,可实现水印的不可见性;另外,根据其第 2 个特性,可以认为对嵌入水印的图像进行某种攻击,对奇异值不会产生大变化,则能有效地保证水印的鲁棒性。

1.2 PCA 分析和 SVD 的关系

PCA 问题实质上是一种变换,经过变换使数据具有较大的方差,方差大的方向是信号的主要方向,方差小的方向是噪声方向或不紧要信号的方向,只保留方差大的方向的数据,就可以对源数据实现近似描述。文献[12]中指出,利用 SVD 可以很方便快捷地实现主成分提取:将式(1)左右两边同时左乘矩阵 $\mathbf{U}^T$, 可得式(4)左式,实现了对原图像列空间的变换,变换矩阵为 $\mathbf{U}^T$, 得到了一个方向的主成分 $\mathbf{Z}$ 。类似可得到另一个主成分。

$$\mathbf{Z} = \mathbf{\Sigma}\mathbf{V}^T \quad \text{或} \quad \mathbf{Z} = \mathbf{U}\mathbf{\Sigma} \quad (4)$$

2 本文算法

2.1 水印嵌入

本文算法在传统的基于 SVD 水印算法的基础上,结合 PCA 对水印图像进行 PC 提取,之后进行了二次分解,过滤掉水印图像对载体图像产生的降质,提高不可见性,支持彩色和灰度图像作为水印图像,不同于大多数的只支持二值图像水印^[3,13],另外支持较大范围的嵌入强度因子,并且不对鲁棒性造成影响。一般来说,为了提高水印安全性,首先对二值水印图像进行加密。如图 1 所示,相同的解密算法用在提取过程。



图 1 水印和加密水印

1) 对载体图像 $\mathbf{I}$ 和水印图像 $\mathbf{W}$ 进行 SVD 分解。

$$\mathbf{I} \Rightarrow \mathbf{U}\mathbf{\Sigma}\mathbf{V}^T \quad \mathbf{W} \Rightarrow \mathbf{U}_w\mathbf{\Sigma}_w\mathbf{V}_w^T \quad (5)$$

2) 采取式(6)的方法计算水印图像的 PC。

$$\mathbf{PC}_w = \mathbf{U}_w\mathbf{\Sigma}_w \quad (6)$$

3) 将水印图像的主成分嵌入到载体图像的奇异值中。

$$\mathbf{\Sigma}_I = \sum + \alpha \mathbf{PC}_w \quad (7)$$

式中: α 为嵌入强度因子。

4) 对嵌入水印的奇异值矩阵再次进行奇异值分解,通过二次分解,可以提高嵌入图像的不可见性,并不对鲁棒性造成影响,能够改善文献[11-10, 14]中存在的嵌入强度因子对不可见性和鲁棒性影响较大的问题。

$$\mathbf{\Sigma}_I \Rightarrow \mathbf{U}_2\mathbf{\Sigma}_2\mathbf{V}_2^T \quad (8)$$

5) 行 SVD 逆变换,得到嵌入水印的图像 $\mathbf{I}_{\text{embed}}$:

$$\mathbf{I}_{\text{embed}} = \mathbf{U}_2\mathbf{\Sigma}_2\mathbf{V}^T \quad (9)$$

2.2 水印提取

水印的提取过程是嵌入的逆过程,经过推导简化可以分为以下 3 步,简化了步骤,精简了算法。

1) 对参考水印图像 $\mathbf{R}$ 进行 SVD 分解。

$$\mathbf{R} \Rightarrow \mathbf{U}_R\mathbf{\Sigma}_R\mathbf{V}_R^T \quad (10)$$

2)得到待提取水印图像的 PC。

$$ExPC_w = \frac{U_2 U^T I^* V V^T - \Sigma}{\alpha} \tag{11}$$

式中： I^* 为可能遭受攻击或未被攻击的嵌入水印的图像。

3)右乘参考水印图像的 V_R^T ，可提取水印。

$$ExWatermark = ExPC_w V_R^T \tag{12}$$

通过这种方式可以实现高不可见性和较好鲁棒性的可靠水印。

3 结果及分析

本文从不可见性、鲁棒性和可靠性分析算法。

3.1 不可见性

常用于测量不可见性的标准是峰值信噪比 (peak signal-to-noise ratio, PSNR)。

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{13}$$

其中，均方误差(mean square error, MSE)是原始图像

和嵌入水印后的图像间的误差计算值。

$$MSE = \frac{1}{N}\left(\sum_{n=1}^N (embed(n) - host(n))\right) \tag{14}$$

其中， N 为图像的总像素数， $embed$ 为嵌入水印后的图像， $host$ 为原始待嵌入水印图像。

PSNR 是一种客观评判标准，在多数情况下并不能真正反映两幅图像的相似程度。可选的另一种测量标准是主观评判标准：结构相似性 (structural similarity index, SSIM)。

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{15}$$

为简洁性表示，其中的 x 和 y 分别代表式 (14) 中的 embed 和 host。

采用 BaboonRGB 为载体图像、彩色图像 LenaRGB、灰度图像 Peppers 和二值图像 shdx 分别为水印图像，与文献[10]中算法进行比较，结果对比如表 1 所示。图 2 所示为不同强度嵌入因子的 PSNR 值折线结果。

表 1 不可见性结果

原始图像 I	水印图像 W	嵌入强度 α	本文嵌入图像 I_{embed}	基于SVD-PCA水印算法嵌入图像 I_{embed}	本文提取水印 $ExWatermark$	基于SVD-PCA水印算法提取水印 $ExWatermark$	本文算法				基于SVD-PCA算法			
							嵌入过程		提取过程		嵌入过程		提取过程	
							PSNR	SSIM	BER	NCC	PSNR	SSIM	BER	NCC
		0.1					55.744 9	1	0.001 3	1	25.725 3	0.925 1	0.693	0.996 5
		0.1					53.295 6	0.999 9	0.001 3	1	26.678 9	0.936 7	0.629 6	0.995 7
	SH DX	10			SH DX	SH DX	54.566 2	0.999 9	0	1	31.951 6	0.979	0	1

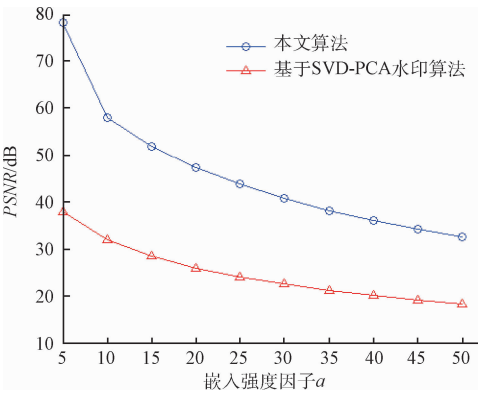


图 2 不可见性对比结果

表 1 中，本文算法对彩色图像、灰度图像、二值图像的水印嵌入效果都实现很好的不可见性，这与一般算法只针对二值图像的算法^[3,13,15]不同，本文算法对水印的选择没有要求。其中，PSNR 高达 55，并能够在不受攻击情况下完全提取出水印。而文献[10]在相同嵌入强度下，不可见

性受到损失，提取的水印不完整，可见，本文的算法在水印的不可见性方面较优。

图 2 中，本文算法(圆圈)的折线要高于文献[10]算法折线(三角)。在相同的嵌入强度因子下，本文提出算法的 PSNR 值要更高，体现更优的不可见性；在同一 PSNR 值下，文献[10]算法可支持的嵌入强度因子较小，本文算法能够支持较大范围的嵌入强度因子。

3.2 鲁棒性

算法的鲁棒性测量从以下两个测量指标体现：归一化相关系数(normalized cross correlation, NCC)和比特错误率(bit error rate, BER)。

$$NCC = \frac{\sum_{n=1}^N ((W(n) - W_m(n))(WEx(n) - WEx_m(n)))}{\sqrt{\sum_{n=1}^N (W(n) - W_m(n))^2} \sqrt{\sum_{n=1}^N (WEx(n) - WEx_m(n))^2}} \tag{16}$$

式中： W 和 W_m 分别为为原始水印和均值， WEx 和 WEx_m

分别为提取的水印和均值。

$$BER = \frac{\sum_{n=1}^N diff |W(n) - WEx(n)|}{N}$$

(17)

式中: N 为总像素数, $diff |W(n) - WEx(n)|$ 为原始水印和提取的水印像素不同的数目。

对嵌入水印的 LenaRGB 图像进行不同攻击,从攻击的

图像中提取水印,与文献[10]算法结果进行对比,如表 2 所示。从表中可以看出,本文算法对 JPEG 压缩、锐化、裁剪、放缩等攻击具有较好的鲁棒性,对模糊、裁剪、图像变亮、加噪等攻击鲁棒性相对较弱,但仍明显强于文献[10]中算法,能对较多的攻击实现鲁棒性,较为完整地提取出水印。

表 2 鲁棒性结果

攻击类型	本文算法 攻击图像	本文算法 提取水印 <i>ExWatermark</i>	基于SVD-PCA水印 算法 提取水印	本文算法 提取过程 <i>BER</i>	本文算法 提取过程 <i>NCC</i>	基于SVD-PCA水印 算法 提取过程 <i>BER</i>	基于SVD-PCA水印 算法 提取过程 <i>NCC</i>	攻击类型	攻击图像	本文算法 提取水印 <i>ExWatermark</i>	基于SVD-PCA水 印算法 提取水印	本文算法 提取过程 <i>BER</i>	本文算法 提取过程 <i>NCC</i>	基于SVD-PCA水印 算法 提取过程 <i>BER</i>	基于SVD-PCA水印 算法 提取过程 <i>NCC</i>
加噪				0.022 71	0.932 49	0.027 83	0.918 74	裁剪,左上 角变白部分, 10%				0.009 52	0.971 54	0.025 63	0.927 43
JPEG 压缩 质量0%				0.017 82	0.947 36	0.367 43	0.210 67	裁剪,左上 角变白部分, 20%				0.033 69	0.904 17	0.081 54	0.786 57
JPEG 压缩 质量40%				0.004 88	0.985 19	0.254 15	0.411 17	裁剪,中心 变白部分, 10%				0.026 37	0.922 82	0.020 26	0.941 19
JPEG 压缩 质量80%				0.00049	0.998 5	0.030 03	0.912 57	裁剪,中心 变白部分, 20%				0.104	0.727 55	0.053 47	0.848 76
均值模糊 blur 3×3				0.00977	0.970 77	0.344 24	0.255 69	缩小为30%				0.024 17	0.929 43	0.433 11	0.099 39
均值模糊 blur 5×5				0.027 59	0.920 72	0.437 26	0.089 42	缩小为40%				0.004 39	0.986 6	0.396 24	0.163 49
均值模糊 blur 9×9				0.082 03	0.781 4	0.478 03	0.029 82	放大为 130%				0	1	0.015 14	0.954 76
运动模糊 45度11个 像素				0.054 2	0.851	0.467 53	0.046 22	放大为 150%				0	1	0.003 91	0.988 07
锐化 锐化因子: 1				0.0117 2	0.965 22	0.163 57	0.589 38	图像变亮				0.077 88	0.796 66	0.157 96	0.615 34

JPEG 压缩是最为常见的无意攻击之一。图 3 以 JPEG 压缩为例,比较了本文算法与文献[10]算法的鲁棒性。图 3 显示本文算法的抗 JPEG 攻击能力较强,在高强度的 JPEG 压缩下仍能保持 NCC 在 0.94 以上;轻微的 JPEG 压缩下,水印能够完整提取。而文献[10]算法对 JPEG 的鲁棒性不如人意,压缩强度越大,水印损坏越大,不能实现水印的鲁棒性要求。

3.3 可靠性

基于 SVD 的水印算法具有虚警问题,本文算法能够很好的解决这个问题,只有正确的参考水印才能提取出水印,伪造的参考图像无法提取水印。以 BaboonRGB 载体图像,彩色图像 LenaRGB、灰度图像 Ship 和二值图像 shdx 分别为水印图像,彩色图像 PeppersRGB、灰度图像 Reference1 图像和二值图像 abcd 分别为参考图像,进行水

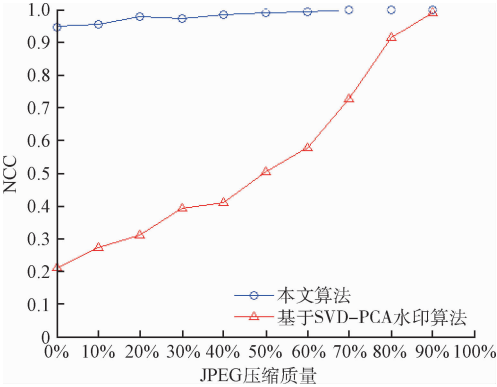
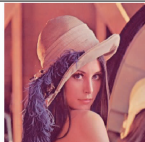
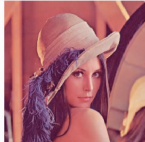
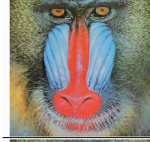
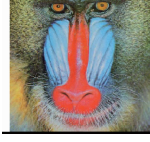


图 3 鲁棒性对比结果

印提取,与文献[7]简化的核心算法结果对比,如表 3 所示。

表 3 可靠性结果

原始图像 I	水印图像 W	参考水印图像 R	本文算法 提取水印 $ExWatermark$	传统基于SVD算法 提取水印 $ExWatermark$	本文算法		传统基于SVD算法	
					提取过程		提取过程	
					BER	NCC	BER	NCC
					0.001 3	1	0.992 4	0.914 3
					0.995 2	0.463	0.994 6	0.363 4
					0.590 5	0.998 4	0.985 1	0.867 6
					0.986	0	0.990 5	0
	SH DX	SH DX	SH DX		0	1	0.058 1	0.778 7
	SH DX	AB CD			0.516 8	0	0.129 2	0.482 8

从表 3 中,根据本文算法,只有参考水印图像与嵌入的原始水印图像相同才能提取出正确的水印,否则提取的水印从肉眼即可分辨不对,另外 BER 和 NCC 值也很好的说明了这点,可见本文算法较好地解决了虚警问题,实现较高的可靠性,并且对于彩色图像、灰度图像、二值图像都可以实现可靠性,其中,对彩色图像的可靠性不如对灰度图像和二值图像,原因在于彩色图像需要进行色彩还原,在色彩还原中,需要借助参考图像的色彩。而文献[7]算法存在与 Liu 同样的较高虚警率问题,利用参考水印图像可以很容易提取出接近参考水印图像的水印图像,受到攻击者伪造版权水印的攻击。

4 结 论

本文算法较为简洁,对之前提出算法进行更多实验的扩充和完善,能实现水印嵌入的较高不可见性,对于彩色图像、灰度图像、二值图像作为水印图像都适用;解决了基于 SVD 算法最大缺点一高虚警问题,实现了可靠水印;另外,通过对嵌入水印的图像认为施加攻击,根据本文算法进行水印提取,能较为完整的提取出水印,满足水印的鲁

棒性要求,在一定程度上能够平衡不可见性和鲁棒性之间的平衡。但是,由于算法为非盲的水印技术,要求版权受侵犯者必须提供可证明身份的原始水印图像,因此在版权保护的应用中具有局限性。

参考文献

[1] 周美丽,白宗文. 基于 HVS 的压缩域数字水印嵌入系统的设计[J]. 国外电子测量技术, 2015 34(4): 78-80.

[2] LOGANATHAN A, KALIYAPERUMAL G. An adaptive HVS based video watermarking scheme for multiple watermarks using BAM neural networks and fuzzy inference system [J]. Expert Systems with Applications An International Journal, 2016, 63(C): 412-434.

[3] 黄修训,周霁婷,张文俊,等. 基于多特征的半脆弱视频水印算法研究[J]. 电子测量技术, 2015, 38(4):58-63.

[4] LAI C C. A digital watermarking scheme based on

- singular value decomposition and tiny genetic algorithm [J]. Digital Signal Processing, 2011, 21(4): 522-527.
- [5] BHATNAGAR G, WU Q M J, RAMAN B. A new robust adjustable logo watermarking scheme [J]. Computers & Security, 2012, 31(1): 40-58.
- [6] LOUKHAOUKHA K. Comments on A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm[J]. Digital Signal Processing, 2013, 23(4): 1334.
- [7] DOGAN S, TUNCER T, AVCI E, et al. A robust color image watermarking with singular value decomposition method[J]. Advances in Engineering Software, 2011, 42(6): 336-346.
- [8] GUO J M, PRASETYO H. Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition[J]. AEU-International Journal of Electronics and Communications, 2014, 68(9): 816-834.
- [9] 吴一全, 史骏鹏, 陶飞翔. 基于 SIFT 和 NMF-SVD 的 NSCT 域抗几何攻击水印算法[J]. 电子测量与仪器学报, 2015, 29 (7): 961-969.
- [10] RUN R S, HORNG S J, LAI J L, et al. An improved SVD-based watermarking technique for copyright protection [J]. Expert Systems with Applications, 2012, 39(1): 673-689.
- [11] LOUKHAOUKHA K, REFAEY A, ZEBBICHE K. Comments on A robust color image watermarking with singular value decomposition method [J]. Advances in Engineering Software, 2016 (93): 44-46.
- [12] SHLENS J. A tutorial on principal component analysis[J]. ARXIV, 2014, arXiv:1404.1100.
- [13] 赵杰. 一种基于 DCT 量化的视频水印算法[J]. 电子测量技术, 2016, 39(6): 72-75.
- [14] GUO J M, PRASETYO H. False-positive-free SVD-based image watermarking [J]. Journal of Visual Communication and Image Representation, 2014, 25(5): 1149-1163.
- [15] 文昌, 金聪, 严盟. 一种 DCT 域子采样的鲁棒可去性盲水印[J]. 电子测量技术, 2012, 35(5): 54-57.

作者简介

王欢欢, 硕士研究生, 研究方向为数字图像、视频水印技术等。

E-mail: 13262559473@163.com

周霁婷, 工学博士, 讲师, 主要研究方向为多媒体通信技术及应用、多媒体数据压缩技术、视频图像处理等。

E-mail: zjting163@163.com