doi:10.3788/gzxb20124102.0210

抗 JPEG 压缩和几何攻击的鲁棒零水印算法

叶天语

(浙江工商大学 信息与电子工程学院,杭州 310018)

摘 要:针对数字图像传输时经常面临 JPEG 压缩和几何攻击,提出一种抗 JPEG 压缩和几何攻击的鲁棒零水印算法.将原始图像分割成互不重叠的子块,对每个子块进行奇异值分解,对奇异值矩阵进行 harr 小波变换,通过比较相邻两个子块奇异值矩阵小波低频逼近子带对角线元素的均值大小关系产生零水印序列.数学理论分析表明:通过比较相邻两个子块奇异值矩阵所有奇异值的均值大小关系产生零水印序列,算法实质上没有对原始图像做任何改动,具有非常好的不可见性.实验结果表明,该算法在抵抗 JPEG 压缩和旋转、尺寸缩放、随机删除行列、偏移行列、打印-扫描几种几何攻击表现出比较强的鲁棒性.

关键词:数字水印;零水印;鲁棒性;JPEG 压缩;几何攻击

中图分类号:TN911.7 **文献标识码**:A **文章编号**:1004-4213(2012)02-0210-8

0 引言

根据数字水印的嵌入位置,数字水印算法可分为空域水印算法和变换域水印算法.变换域主要有奇异值分解(Singular Value Decomposition, SVD),离散小波变换(Discreet Wavelet Transformation, DWT),离散余弦变换(Discreet Cosine Transformation, DCT)等.一些学者提出将水印嵌入在单一的 SVD 域或 DWT 域以实现对数字图像进行版权保护.文献[1]利用奇异值的稳定性将高斯分布伪随机数序列作为水印嵌入在原始载体图像的奇异值中;文献[2]分析了图像经 DWT 后产生的各小波子带系数的特点,提出首先将水印嵌入在小波低频子带再将剩余水印嵌入在小波高频子带的嵌入策略;文献[3]结合温泉等[4]提出的零水印技术,提出利用图像子块最大奇异值最高位数字奇偶性产生零水印序列.一些学者还提出将水印嵌入在 SVD 和 DWT 的混合域.文献[5]首先对图像进行 DWT,然后利用小波低频子带每个分块最大奇异值的最高位数字奇偶性产生零水印序列;文献[6]首先对图像进行 DWT,然后利用小波低频子带相邻两个分块的最大奇异值数值大小比较产生二进制嵌入密钥矩阵,再与原始二值图像异或产生零水印;文献[7]首先将原始图像进行分块,再对每个子块进行 DWT,对小波低频子带进行 SVD,将二值图像水印量化嵌入最大奇异值;文献[8]将原始载体图像分成四个相同大小的子块并对每个子块进行 DWT,将灰度水印图像的奇异值加性嵌入在四个子块的小波低频子带的奇异值中;文献[9]将原始水印图像和原始载体图像分别进行 DWT 并将得到的所有小波子带进行 SVD,再将水印图像各个小波子带的奇异值加性嵌入到原始图像对应小波子带的奇异值中.

数字图像在互联网中传播可能会面临多种攻击,其中 JPEG 压缩和几何攻击是比较常见的攻击.JPEG 压缩是国际上通用的一种图像压缩标准,用于攻击图像将具有很强的针对性;几何攻击会造成嵌入的水印去同步使得检测端无法正确判断出水印嵌入的位置,往往具有很强的攻击性.数字图像水印算法是否具有抵抗 JPEG 压缩和几何攻击的鲁棒性是衡量其实用性的一个指标.但是,上述水印算法在抵抗以上几何攻击上并不都具有很强的鲁棒性.总体上看,文献[1-2,7-8]在抵抗以上几何攻击上具有较差的鲁棒性;文献[3,5-6,9]具有一定的抵抗以上几何攻击的鲁棒性,但还有待进一步提高.

基于以上分析,本文提出一种基于 SVD 和 DWT 的抗 JPEG 压缩和几何攻击的鲁棒零水印算法.算法将图像分割成互不重叠的子块,对每个子块进行 SVD,对奇异值矩阵进行 harr 小波变换,通过比较相邻两个子块奇异值矩阵小波低频逼近子带对角线元素的均值大小关系产生零水印序列.实验结果表明该算法在抵抗 JPEG 压缩和几何攻击上表现出比较强的鲁棒性.

1 原始零水印序列产生算法

原始图像的大小为 $N\times N$,其中 $N=2^n$,n 为正整数.根据以下步骤从原始图像产生原始零水印

基金项目:浙江省教育厅项目(No. Y201017916)资助

作者简介:叶天语(1982—),男,讲师,工学博士,主要研究方向为信息隐藏与数字水印. Email: flystu008@yahoo.com.cn

收稿日期:2011-07-28;**修回日期**:2011-10-19

序列:

Step1:将原始图像分割成互不重叠的大小为 $M\times M$的子块,其中 $M=2^m$,m 为正整数;

Step2:对每个子块进行 SVD,第 k 个子块的奇异值矩阵记为 S_k,$k=1,2,\cdots\left(\frac{N}{M}\right)^2$;

Step3:对 S_k 进行 l 级 harr 小波变换,得到小波低频逼近子带;

Step4:对小波低频逼近子带的对角线元素进行均值计算,将得到的均值记为 η_k;

Step5:通过比较相邻两个子块的 η_k 的大小关系产生原始零水印序列 W. 即:如果 $\eta_{2t-1}\geqslant\eta_{2t}$,则令 $w_t=0$;反之,令 $w_t=1$. 其中,w_t 为 W 的第 t 比特水印,$t=1,2,\cdots\frac{1}{2}\left(\frac{N}{M}\right)^2$.

2　零水印序列提取算法

根据以下步骤从大小为 $N\times N$ 的攻击后的图像提取零水印序列:

Step1:将攻击后的图像分割成互不重叠的大小为 $M\times M$ 的子块;

Step2:对每个子块进行 SVD,第 k 个子块的奇异值矩阵记为 S_k^a,$k=1,2,\cdots,\left(\frac{N}{M}\right)^2$;

Step3:对 S_k^a 进行 l 级 harr 小波变换,得到小波低频逼近子带;

Step4:对小波低频逼近子带的对角线元素进行均值计算,将得到的均值记为 η_k^a;

Step5:通过比较相邻两个子块 η_k^a 的大小关系提取零水印序列 W^a. 即:如果 $\eta_{2t-1}^a\geqslant\eta_{2t}^a$,则令 $w_t^a=0$;反之,令 $w_t^a=1$. 其中,w_t^a 为 W^a 的第 t 比特水印,$t=1,2,\cdots,\frac{1}{2}\left(\frac{N}{M}\right)^2$.

Step6:计算原始零水印序列 W 和从攻击图像提取的零水印序列 W^a 之间的相似度评价抗攻击鲁棒性以判断版权. 相似度定义为

$$\lambda=1-\left[\sum_{t=1}^{\frac{1}{2}\left(\frac{N}{M}\right)^2}w_t\oplus w_t^a\right]/\left[\frac{1}{2}\left(\frac{N}{M}\right)^2\right]\tag{1}$$

3　算法的数学理论分析

每个大小为 $M\times M$ 的子块进行 SVD 得到奇异值矩阵 S,将 S 的每个元素记为 s_{ij},其中 $i=1,2,\cdots,M$ 和 $j=1,2,\cdots,M$,即

$$S=\begin{bmatrix}s_{11}&s_{12}&\cdots&s_{1M}\\s_{21}&s_{22}&\cdots&s_{2M}\\\vdots&\vdots&\ddots&\vdots\\s_{M_1}&s_{M_2}&\cdots&s_{MM}\end{bmatrix}_{M\times M}.$$

文献[10]的附录部分利用滤波器组方法证明了 harr 小波变换低频逼近子带系数与图像块直接相关. 本文认为通过直接对图像空域像素进行分块均值计算可以得到与文献[10]附录部分同样的结论. 接下来运用分块均值计算推导奇异值矩阵 S 的 l 级 harr 小波变换低频逼近子带.

对 S 按照式(2)进行 2×2 分块均值计算,将所得矩阵记为 S_1、S_1 的每个元素记为 s_{ij}^1,即

$$S_1=\begin{bmatrix}s_{11}^1&s_{12}^1&\cdots&s_{1\frac{M}{2}}^1\\s_{21}^1&s_{22}^1&\cdots&s_{2\frac{M}{2}}^1\\\vdots&\vdots&\ddots&\vdots\\s_{\frac{M}{2}1}^1&s_{\frac{M}{2}2}^1&\cdots&s_{\frac{M}{2}\frac{M}{2}}^1\end{bmatrix}_{\frac{M}{2}\times\frac{M}{2}}=\frac{1}{2^1}\begin{bmatrix}\sum_{i=1}^{2}\sum_{j=1}^{2}s_{ij}&\sum_{i=1}^{2}\sum_{j=3}^{4}s_{ij}&\cdots&\sum_{i=1}^{2}\sum_{j=M-1}^{M}s_{ij}\\\sum_{i=3}^{4}\sum_{j=1}^{2}s_{ij}&\sum_{i=3}^{4}\sum_{j=3}^{4}s_{ij}&\cdots&\sum_{i=3}^{4}\sum_{j=M-1}^{M}s_{ij}\\\vdots&\vdots&\ddots&\vdots\\\sum_{i=M-1}^{M}\sum_{j=1}^{2}s_{ij}&\sum_{i=M-1}^{M}\sum_{j=3}^{4}s_{ij}&\cdots&\sum_{i=M-1}^{M}\sum_{j=M-1}^{M}s_{ij}\end{bmatrix}_{\frac{M}{2}\times\frac{M}{2}}=$$

$$\frac{1}{2^1}\begin{bmatrix}\sum_{i=1}^{2}\sum_{j=1}^{2}s_{ij}&0&\cdots&0\\0&\sum_{i=3}^{4}\sum_{j=3}^{4}s_{ij}&\cdots&0\\\vdots&\vdots&\ddots&0\\0&0&0&\sum_{i=M-1}^{M}\sum_{j=M-1}^{M}s_{ij}\end{bmatrix}_{\frac{M}{2}\times\frac{M}{2}}=\frac{1}{2^1}\begin{bmatrix}\sum_{i=1}^{2}\sigma_i&0&\cdots&0\\0&\sum_{i=3}^{4}\sigma_i&\cdots&0\\\vdots&\vdots&\ddots&0\\0&0&0&\sum_{i=M-1}^{M}\sigma_i\end{bmatrix}_{\frac{M}{2}\times\frac{M}{2}}\tag{2}$$

可见,式(2)对角线元素为子块奇异值矩阵每 2 个相邻奇异值的均值.

依此类推,对 S 按照式(3)进行 $2^l\times2^l$ 分块均值计算,将所得矩阵记为 S_l、S_l 的每个元素记为 s_{ij}^l,即

$$S_l=\begin{bmatrix} s_{11}^l & s_{12}^l & \cdots & s_{1\frac{M}{2^l}}^l \\ s_{21}^l & s_{22}^l & \cdots & s_{2\frac{M}{2^l}}^l \\ \vdots & \vdots & \ddots & \vdots \\ s_{\frac{M}{2^l}1}^l & s_{\frac{M}{2^l}2}^l & \cdots & s_{\frac{M}{2^l}\frac{M}{2^l}}^l \end{bmatrix}_{\frac{M}{2^l}\times\frac{M}{2^l}}=\frac{1}{2^l}\begin{bmatrix} \sum_{i=1}^{2^l}\sum_{j=1}^{2^l}s_{ij} & \sum_{i=1}^{2^l}\sum_{j=2^l+1}^{2^{l+1}}s_{ij} & \cdots & \sum_{i=1}^{2^l}\sum_{j=M-2^l+1}^{M}s_{ij} \\ \sum_{i=2^l+1}^{2^{l+1}}\sum_{j=1}^{2^l}s_{ij} & \sum_{i=2^l+1}^{2^{l+1}}\sum_{j=2^l+1}^{2^{l+1}}s_{ij} & \cdots & \sum_{i=2^l+1}^{2^{l+1}}\sum_{j=M-2^l+1}^{M}s_{ij} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=M-2^l+1}^{M}\sum_{j=1}^{2^l}s_{ij} & \sum_{i=M-2^l+1}^{M}\sum_{j=2^l+1}^{2^{l+1}}s_{ij} & \cdots & \sum_{i=M-2^l+1}^{M}\sum_{j=M-2^l+1}^{M}s_{ij} \end{bmatrix}_{\frac{M}{2^l}\times\frac{M}{2^l}}=$$

$$\frac{1}{2^l}\begin{bmatrix} \sum_{i=1}^{2^l}\sum_{j=1}^{2^l}s_{ij} & 0 & \cdots & 0 \\ 0 & \sum_{i=2^l+1}^{2^{l+1}}\sum_{j=2^l+1}^{2^{l+1}}s_{ij} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sum_{i=M-2^l+1}^{M}\sum_{j=M-2^l+1}^{M}s_{ij} \end{bmatrix}_{\frac{M}{2^l}\times\frac{M}{2^l}}=\frac{1}{2^l}\begin{bmatrix} \sum_{i=1}^{2^l}\sigma_i & 0 & \cdots & 0 \\ 0 & \sum_{i=2^l+1}^{2^{l+1}}\sigma_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sum_{i=M-2^l+1}^{M}\sigma_i \end{bmatrix}_{\frac{M}{2^l}\times\frac{M}{2^l}} \tag{3}$$

可见，式(3)对角线元素为子块奇异值矩阵每 2^l 个相邻奇异值的均值，而且 S_l 就是 S 的 l 级 harr 小波变换低频逼近子带. 至此，完成了推导 S 的 l 级 harr 小波变换低频逼近子带的过程.

对 S_l 的对角线元素按照式(4)再进行均值计算，所得结果为 η，即

$$\eta=\frac{1}{\left(\frac{M}{2^l}\right)}\times\left(\sum_{i=1}^{2^l}\frac{\sigma_i}{2^l}+\sum_{i=2^l+1}^{2^{l+1}}\frac{\sigma_i}{2^l}+\cdots+\sum_{i=M-2^l+1}^{M}\frac{\sigma_i}{2^l}\right)=$$

$$\frac{1}{\left(\frac{M}{2^l}\right)}\times\left(\sum_{i=1}^{M}\frac{\sigma_i}{2^l}\right)=\frac{1}{M}\times\left(\sum_{i=1}^{M}\sigma_i\right) \tag{4}$$

可见，η 为子块奇异值矩阵所有奇异值的均值. 这表明算法实质上是通过比较相邻两个子块奇异值矩阵所有奇异值的均值的大小关系产生零水印序列. 另外，根据式(4)，零水印序列的产生只与图像分块大小 M 和每个子块的奇异值 σ_i 有关，与 harr 小波变换级数 l 无关.

4 实验结果

4.1 阈值选择

Lena、Peppers、Baboon、Frog、Elain、Boat 是六幅大小都是 512×512 的 256 灰度级图像，分别见图 1～6. 图像子块的大小为 32×32，harr 小波分解级数为3级，所以零水印序列长度为128 bit. 六幅图像原始零水印序列之间的相似度见表 1. 从表 1 可见，六幅不同图像原始零水印序列之间的相似度最大值为 0.554 7，最小值为 0.437 5.

图1 Lena
Fig.1 Lena

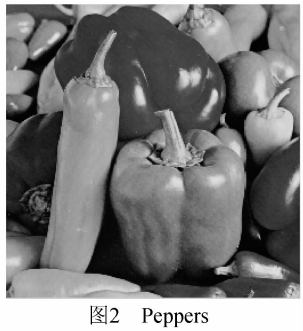

图2 Peppers
Fig.2 Peppers

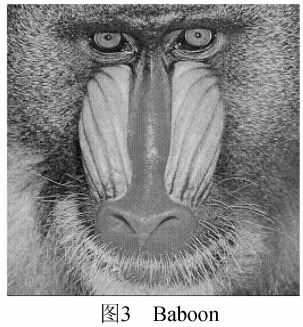

图3 Baboon
Fig.3 Baboon

图4 Frog
Fig.4 Frog

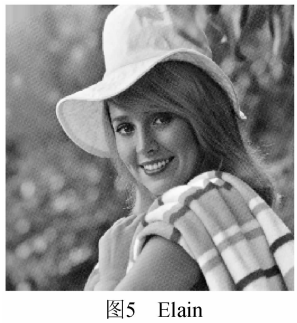

图5 Elain
Fig.5 Elain

图6 Boat
Fig.6 Boat

表 1　不同图像原始零水印序列之间的相似度

Table 1　Similarities between the original zero-watermark sequences from different images

	Lena	Peppers	Baboon	Frog	Elain	Boat
Lena	1	0.539 1	0.484 4	0.507 8	0.554 7	0.523 4
Peppers	0.539 1	1	0.476 6	0.531 3	0.437 5	0.484 4
Baboon	0.484 4	0.476 6	1	0.460 9	0.476 6	0.460 9
Frog	0.507 8	0.531 3	0.460 9	1	0.453 1	0.500 0
Elain	0.554 7	0.437 5	0.476 6	0.453 1	1	0.484 4
Boat	0.523 4	0.484 4	0.460 9	0.500 0	0.484 4	1

Lena 图像的原始零水印序列与 599 个{0,1}随机均匀分布序列之间的相似度见图 7,其中第 300 个是 Lena 图像原始零水印序列.从图 7 可见,相似度基本上在 0.5 附近波动.其他图像的原始零水印序列与{0,1}随机均匀分布序列之间的相似度具有类似的结论.限于篇幅,这里不一一列出.综合上述分析,认为选择 0.80 作为阈值已经足够大.

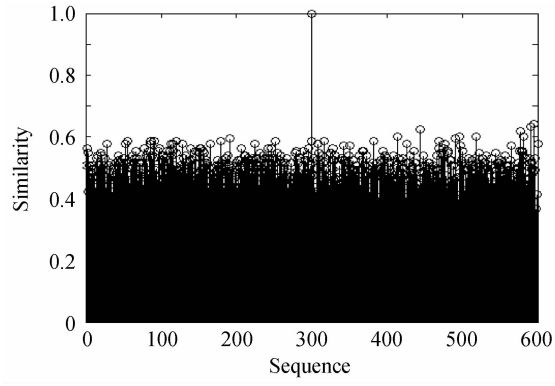

图 7　Lena 图像原始零水印序列与{0,1}随机均匀分布序列之间的相似度

Fig. 7　Similarities between the original zero-watermark sequence from Lena and random uniform {0,1} sequences

4.2　抗 JPEG 压缩和几何攻击鲁棒性测试

以图 1 的 Lena 图像为实验图像测试算法抵抗 JPEG压缩和几何攻击的鲁棒性.图像子块的大小为 32×32,haar 小波分解级数为 3 级.几何攻击包括旋转、尺寸缩放、随机删除行列、偏移行列、打印-扫描.各表中"/"上方为原始零水印序列与攻击后提取的零水印序列之间的相似度,"/"下方为原始 Lena 图像与攻击后的 Lena 图像之间的 PSNR.

4.2.1　JPEG 压缩

对图 1 的原始 Lena 图像 JPEG 压缩,实验参量和结果见表 2.由表 2 可见,尽管质量因子已经比较小,相似度仍然很高,所以算法抗 JPEG 压缩鲁棒性很强.

表 2　JPEG 压缩

Table 2　JPEG compression

	Quality factor				
	40	30	20	10	5
This paper(l=3)	1.000 0/34.800 8	0.992 2/33.952 4	0.992 2/32.633 1	0.984 4/30.087 8	0.960 9/27.007 0
This paper(l=4)	1.000 0/34.800 8	0.992 2/33.952 4	0.992 2/32.633 1	0.984 4/30.087 8	0.960 9/27.007 0
Reference[3]	0.978 3/34.800 8	0.970 5/33.952 4	0.959 2/32.633 1	0.918 5/30.087 8	0.818 1/27.007 0
Reference[5]	0.996 1/34.800 8	0.996 1/33.952 4	0.988 3/32.633 1	0.980 5/30.087 8	0.953 1/27.007 0
Reference[6]	0.988 3/34.800 8	0.986 3/33.952 4	0.964 8/32.633 1	0.954 1/30.087 8	0.897 5/27.007 0
Reference[7]	0.928 7/33.376 1	0.838 9/32.733 4	0.764 6/31.7094	0.662 1/29.532 0	0.528 3/26.760 6
Reference[11]	1.000 0/34.800 8	0.989 0/33.952 4	0.990 5/32.633 1	0.989 0/30.087 8	0.953 1/27.007 0

4.2.2　几何攻击

1)旋转

将原始 Lena 图像逆时针旋转,实验参量和结果见表 3.由表 3 可见,算法能够抵抗旋转攻击.

表 3　逆时针旋转

Table 3　Anticlockwise rotation

	Angle		
	1	2	2.5
This paper(l=3)	0.921 9/20.915 7	0.875 0/17.785 9	0.843 8/16.880 2
This paper(l=4)	0.921 9/20.915 7	0.875 0/17.785 9	0.843 8/16.880 2
Reference[3]	0.851 6/20.915 7	0.810 5/17.785 9	0.783 9/16.880 2
Reference[5]	0.914 1/20.915 7	0.804 7/17.785 9	0.777 3/16.880 2
Reference[6]	0.907 2/20.915 7	0.846 7/17.785 9	0.825 2/16.880 2
Reference[7]	0.578 1/20.833 4	0.557 6/17.741 8	0.544 9/16.843 0
Reference[11]	0.939 7/20.915 7	0.894 0/17.785 9	0.874 5/16.880 2

2)尺寸缩放

将原始 Lena 图像使用 nearest 插值法进行尺寸缩放,实验参量和结果见表 4. 由表 4 可见,算法具有很强的抵抗尺寸缩放攻击的鲁棒性.

表 4 尺寸缩放

Table 4 Scaling

	Proportion	
	First lessen to 80%, then magnify to 125%	First lessen to 50%, then magnify to 200%
This paper(l=3)	0.992 2/25.713 5	0.984 4/27.967 9
This paper(l=4)	0.992 2/25.713 5	0.984 4/27.967 9
Reference[3]	0.920 2/25.713 5	0.929 7/27.967 9
Reference[5]	0.937 5/25.713 5	0.964 8/27.967 9
Reference[6]	0.960 0/25.713 5	0.961 9/27.967 9
Reference[7]	0.689 5/25.437 5	0.730 5/27.680 8
Reference[11]	0.98 17/25.713 5	0.983 6/27.967 9

3)随机删除行列

对原始 Lena 图像随机删除行. 随机删除行是指从被删除行的下边第一行开始逐行向上移动,空余行补全黑. 实验参量和结果见表 5.

对原始 Lena 图像随机删除列. 随机删除列是指从被删除列的右边第一列开始逐列向左移动,空余列补全黑. 实验参量和结果见表 6.

表 5 随机删除行

Table 5 Random row removal

	Row number		
	6	12	18
This paper(l=3)	0.960 9/20.128 5	0.937 5/17.706 7	0.921 9/16.321 1
This paper(l=4)	0.960 9/20.128 5	0.937 5/17.706 7	0.921 9/16.321 1
Reference[3]	0.867 9/20.128 5	0.828 6/17.706 7	0.819 1/16.321 1
Reference[5]	0.910 2/20.128 5	0.839 8/17.706 7	0.820 3/16.321 1
Reference[6]	0.935 5/20.128 5	0.899 4/17.706 7	0.863 3/16.321 1
Reference[7]	0.706 1/20.071 0	0.739 3/17.675 2	0.716 8/16.301 7
Reference[11]	0.948 0/20.128 5	0.907 5/17.706 7	0.877 0/16.321 1

表 6 随机删除列

Table 6 Random column removal

	Column number		
	2	4	6
This paper(l=3)	0.984 4/23.970 1	0.929 7/20.450 3	0.906 3/18.613 4
This paper(l=4)	0.984 4/23.970 1	0.929 7/20.450 3	0.906 3/18.613 4
Reference[3]	0.933 1/23.970 1	0.908 2/20.450 3	0.890 4/18.613 4
Reference[5]	0.937 5/23.970 1	0.890 6/20.450 3	0.847 7/18.613 4
Reference[6]	0.948 2/23.970 1	0.913 1/20.450 3	0.870 1/18.613 4
Reference[7]	0.761 7/23.832 7	0.716 8/20.387 3	0.713 9/18.571 7
Reference[11]	0.971 7/23.970 1	0.945 1/20.450 3	0.926 0/18.613 4

由表 5 和表 6 可见,算法具有很强的抵抗随机删除行列攻击的鲁棒性.

4)偏移行列

对原始 Lena 图像向下偏移行. 向下偏移行是指将整个图像下移几行,上面几行补全黑,最后几行移出丢失. 实验参量和结果见表 7.

表 7 向下偏移行

Table 7 Downward shifting

	Row number		
	3	6	9
This paper(l=3)	0.984 4/21.620 1	0.968 8/18.703 3	0.914 1/17.194 3
This paper(l=4)	0.984 4/21.620 1	0.968 8/18.703 3	0.914 1/17.194 3
Reference[3]	0.869 4/21.620 1	0.830 1/18.703 3	0.797 4/17.194 3
Reference[5]	0.910 2/21.620 1	0.832 0/18.703 3	0.769 5/17.194 3
Reference[6]	0.949 2/21.620 1	0.914 1/18.703 3	0.878 9/17.194 3
Reference[7]	0.632 8/21.546 0	0.563 5/18.669 1	0.546 9/17.172 6
Reference[11]	0.952 4/21.620 1	0.922 4/18.703 3	0.890 6/17.194 3

对原始 Lena 图像向右偏移列. 向右偏移列是指整个图像右移后,左边几列补全黑,最后几列移出丢失. 实验参量和结果见表 8.

表 8　向右偏移列

Table 8　Right shifting

	Column number			
	2	3	4	5
This paper(l=3)	0.976 6/21.992 8	0.953 1/20.006 4	0.906 3/18.746 6	0.882 8/17.828 7
This paper(l=4)	0.976 6/21.992 8	0.953 1/20.006 4	0.906 3/18.746 6	0.882 8/17.828 7
Reference[3]	0.840 3/21.992 8	0.818 8/20.006 4	0.806 6/18.746 6	0.791 5/17.828 7
Reference[5]	0.925 8/21.992 8	0.863 3/20.006 4	0.800 8/18.746 6	0.761 7/17.828 7
Reference[6]	0.935 5/21.992 8	0.897 5/20.006 4	0.872 1/18.746 6	0.845 7/17.828 7
Reference[7]	0.531 3/21.897 6	0.528 3/19.942 3	0.512 7/18.695 9	0.526 4/17.785 6
Reference[11]	0.960 0/21.992 8	0.945 8/20.006 4	0.929 7/18.746 6	0.909 7/17.828 7

由表 7 和表 8 可见,算法具有很强的抵抗偏移行列攻击的鲁棒性.

5)打印-扫描

打印-扫描及后处理的过程如下:

a1:用 Canon L11121E 激光打印机和 A4 纸将原始 Lena 图像打印出来;

a2:用分辨率设置为 400 dpi 的 CanoScan LiDE 100 扫描仪扫描打印出来的 Lena 图像;

a3:用 Photoshop 将扫描后的 Lena 图像裁剪和旋转校正,调整采样分辨率为 72 dpi,用 bilinear 插值法将大小调整成 512×512 等.

实验结果见表 9. 由表 9 可见,算法抗打印-扫描的鲁棒性很强.

表 9　打印-扫描

Table 9　Print-and-scan

	Print-and-scan
This paper(l=3)	0.929 7/19.313 1
This paper(l=4)	0.929 7/19.313 1
Reference[3]	0.749 0/19.313 1
Reference[5]	0.593 8/19.313 1
Reference[6]	0.865 2/19.313 1
Reference[7]	0.501 0/19.208 6
Reference[11]	0.903 8/19.313 1

以上实验结果表明,算法在抵抗 JPEG 压缩和各种几何攻击上表现出比较强的鲁棒性.

4.3　实验结果分析与讨论抗

4.3.1　harr 小波分解级数对抗攻击鲁棒性的影响

从第 3 部分的数学理论分析可知,零水印序列 W 的产生与 harr 小波分解级数 l 无关,因此 W 和 W^a 之间的相似度也与 l 无关,相应地,本文算法的抗攻击鲁棒性也与 l 无关. 为了从实验结果验证这一点,表 2～9 列出了当 l=4 时本文算法的抗攻击鲁棒性. 对比表 2～9"本文算法 l=3"栏和"本文算法 l=4"栏可知,不管 l=3 还是 l=4,本文算法在抵抗上述攻击的鲁棒性都完全一样. 因为 $M=2^m$ 且 m 为正整数,所以 l 可以取值为小于等于 m 的任何正整数.

4.3.2　与其他算法抗攻击鲁棒性的对比

文献[3,5-6,11]算法都是零水印算法,与本文的零水印算法通过相似度进行抗攻击鲁棒性对比. 文献[3]算法的子块大小为 8×8;文献[5]算法以 harr 小波为基对原始载体图像 Lena 进行 3 级 DWT,子块的大小为 4×4;文献[6]算法以图 8 所示的大小为 32×32 的二值图像 Hand 作为原始水印图像,以 harr 小波为基对原始载体图像 Lena 进行 2 级 DWT,子块大小为 4×4;文献[11]算法的子块大小为 8×8. 文献[3,5-6,11]算法的抗攻击鲁棒性实验结果分别见表 2-9 的相应栏. 对比表 2-9 的实验结果可知,本文算法在抵抗 JPEG 压缩和各种几何攻击上的鲁棒性都明显强于文献[3]和[5]的算法;本文算法在抵抗 JPEG 压缩和各种几何攻击上的鲁棒性都强于文献[6]算法,这是因为本文算法的 harr 小波变换实质上是对子块的奇异值进行操作,而文献[6]算法的 harr 小波变换是对原始载体图像的原始像素进行操作;本文算法在抵抗 JPEG 压缩、尺寸缩放、随机删除行、向下偏移行、打印-扫描、删除列数较少的随机删除列、偏移列数较少的向右偏移列上的鲁棒性强于文献[11]的算法,但在抵抗旋转、删除列数较多的随机删除列、偏移列数较多的向右偏移列上的鲁棒性稍弱于文献[11]的算法,所以总体上可以认为本文算法的抗攻击鲁棒性强于文献[11]的算法.

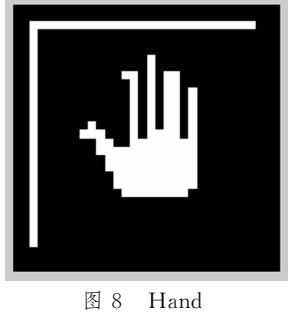

图 8　Hand

Fig. 8　Hand

将文献[7]算法与本文算法进行抗攻击鲁棒性对比. 文献[7]算法设置如下:以图 8 的二值图像

Hand 作为原始水印图像，将原始载体图像 Lena 分割成大小为 16×16 的不重叠子块，以 harr 小波为基对每个子块进行 1 级 DWT，量化步长 Q 为 130. 原始载体图像和含水印图像之间的 PSNR 为 38.881 8 dB，因此此时文献[7]算法具有良好的不可见性. 此时文献[7]算法抗攻击鲁棒性实验结果分别见表 2～9 的相应栏. 对比表 2～9 的实验结果可知，此时文献[7]算法在抵抗 JPEG 压缩和各种几何攻击上的鲁棒性都明显差于本文算法. 另外，文献[7]算法将外在水印嵌入原始图像，由于零水印算法并没有对原始载体图像做任何修改[4]，因此本文算法的不可见性好于文献[7]算法.

5 结论

数字图像在互联网传输时经常面临 JPEG 压缩和几何攻击. 为了解决数字图像在传输过程的版权保护问题，本文提出一种基于 SVD 和 DWT 的抗 JPEG 压缩和几何攻击的鲁棒零水印算法. 数学理论分析表明，本文算法实质上是通过比较相邻两个子块奇异值矩阵所有奇异值的均值的大小关系产生零水印序列. 算法实质上没有对原始图像做任何改动，具有非常好的不可见性. 实验结果表明算法在抵抗 JPEG 压缩和旋转、尺寸缩放、随机删除行列、偏移行列、打印-扫描几种几何攻击表现出比较强的鲁棒性.

参考文献

[1] LIU Rui-zhen, TAN Tie-niu. SVD based digital watermarking method[J]. *Acta Electronica Sinica*, 2001, **29**(2): 168-171.
刘瑞祯，谭铁牛. 基于奇异值分解的数字图像水印算法[J]. 电子学报，2001，**29**(2)：168-171.

[2] HUANG Da-ren, LIU Jiu-fen. An embedding strategy and algorithm for image watermarking in DWT domain [J]. *Journal of Software*, 2002, **13**(7): 1290-1297.
黄达人，刘九芬. 小波变换域图像水印嵌入对策和算法[J]. 软件学报，2002，**13**(7)：1290-1297.

[3] YE Tian-yu, MA Zhao-feng, NIU Xin-xin, *et al*. A robust zero-watermark algorithm based on singular value decomposition for digital right management[C]. Proceedings of the 2nd International Conference on Image and Signal Processing (CISP 2009), Tianjin, China, 2009, 3: 1444-1446.

[4] WEN Quan, SUN Tan-feng, WANG Shu-xun. Concept and application of zero-watermark[J]. *Acta Electronica Sinica*, 2003, **31**(2): 214-216.
温泉，孙锬锋，王树勋. 零水印的概念与应用[J]. 电子学报，2003，**31**(2)：214-216.

[5] YE Tian-yu, MA Zhao-feng, NIU Xin-xin, *et al*. A zero-watermark technology with strong robustness[J]. *Journal of Beijing University of Posts and Telecommunications*, 2010, **33**(3): 126-129.
叶天语，马兆丰，钮心忻，等. 强鲁棒零水印技术[J]. 北京邮电大学学报，2010，**33**(3)：126-129.

[6] ZHOU Ya-xun, JIN Wei. A novel image zero-watermarking scheme based on DWT-SVD[C]. Proceedings of the 2011 International Conference on Multimedia Technology (ICMT 2011), Hangzhou, China, 2011, 2873-2876.

[7] HU Juan, YANG Ge-lan, YAN Quan-feng. Robust blind watermarking algorithm combining DWT and SVD [J]. *Journal of Engineering Graphics*, 2008, (4): 107-110.
胡娟，杨格兰，严权锋. 结合 DWT 和 SVD 的鲁棒盲水印算法[J]. 工程图学学报，2008，(4)：107-110.

[8] XU Xiao-yong, LI Ying. A digital watermarking algorithm based on the combination of DWT and SVD[J]. *Journal of Southwest University for Nationalities. Natural Science Edition*, 2007, **33**(5): 1029-1034.

[9] LI Xiao-fei, CAI Xiang-yun. A robust image watermarking based on DWT - SVD domain [J]. *Journal of Yunnan University*, 2005, **27**(5A): 337-341.
李晓飞，蔡翔云. 基于 DWT-SVD 的图像水印算法[J]. 云南大学学报(自然科学版)，2005，**27**(5A)：337-341.

[10] CHE Sheng-bing, HUANG Da, LI Guang. Semi-fragile image watermarking algorithm based on visual features [J]. *Journal on Communications*, 2007, **28**(10): 134-140.
车生兵，黄达，李光. 基于视觉特性的半脆弱水印算法[J]. 通信学报，2007，**28**(10)：134-140.

[11] YE Tian-yu. A robust zero-watermarking algorithm against dual print-and-scan process based on discrete cosine transformation[J]. *Acta Photonica Sinica*, 2011, **40**(1): 142-148.
叶天语. 离散余弦变换域抗二次打印-扫描鲁棒零水印算法[J]. 光子学报，2011，**40**(1)：142-148.

[12] WANG Xiang-yang, HOU Li-min, WU Jun. A feature-based robust digital image watermarking against geometric attacks [J]. *Image and Vision Computing*, 2008, **26**(7): 980-989.

[13] WANG Xiang-yang, YANG Yi-ping, YANG Hong-ying. Invariant image watermarking using multi-scale Harris detector and wavelet moments[J]. *Computers and Electrical Engineering*, 2010, **36**(1): 31-44.

[14] DENG Cheng, GAO Xin-bo. Geometrically robust image watermarking based on SIFT feature regions [J]. *Acta Photonica Sinica*, 2009, **38**(4): 1005-1010.
邓成，高新波. 基于 SIFT 特征区域的抗几何攻击图像水印算法[J]. 光子学报，2009，**38**(4)：1005-1010.

A Robust Zero-watermarking Algorithm Resisting JPEG Compression and Geometric Attacks

YE Tian-yu

(*College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou* 310018, *China*)

Abstract: A robust zero-watermarking algorithm resisting JPEG compression and geometric attacks is proposed, since digital images always face with JPEG compression and geometric attacks through transmission. An original image is split into non-overlapping blocks, and each block is conducted with singular value decomposition. Then, each block′s singular value matrix is transformed with Harr wavelet transformation. The zero-watermark sequence is produced by judging the numerical relation between the mean of diagonal elements of singular value matrix′s low frequency band from two adjacent blocks. The mathematical theoretical analysis shows that the zero-watermark sequence is essentially produced by judging the numerical relation between the mean of singular value matrix′s singular values from two adjacent blocks. The proposed algorithm has perfect visibility due to no alteration made to the original image. The experimental results show that the proposed algorithm has strong robustness to resist JPEG compression and several geometric attacks such as rotation, scaling, random row & column removal, row & column shifting, print-and-scan.

Key words: Digital watermarking; Zero-watermarking; Robustness; JPEG compression; Geometric attack