基于DWT-SVD的奇异向量量化水印算法

胡 青[1,2] 龙冬阳[1]

(中山大学信息科学与技术学院 广州 510275)[1] (中山大学数学与计算科学学院 广州 510275)[2]

摘 要 提出了一种新颖的可用于版权保护的小波奇异值分解的量化水印算法。与传统的水印比特信息直接嵌入小波系数不同,水印信息被量化嵌入原始图像小波低频子带分块奇异值分解得到的奇异向量中。水印提取无需原始图像,可在密钥和量化阈值控制下实现盲提取。实验表明,含水印图像质量好且能较好地抵抗常规的图像处理,对JPEG压缩具有优异的鲁棒性。

关键词 水印,小波分解,奇异值分解,奇异向量量化

Singular Vector Quantization Watermarking Scheme Based on DWT-SVD

HU Qing[1,2] LONG Dong-yang[1]

(School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China)[1]

(School of mathematics and Computational Science, Sun Yat-Sen University, Guangzhou 510275, China)[2]

Abstract A novel watermarking scheme was proposed for image authentication by applying a simple quantization process on wavelet domain singular value decomposition. Unlike the traditional wavelet-based watermarking schemes where the watermark bits were embedded directly on the wavelet coefficients, the singular vectors of the blocks within wavelet low frequency sub-band of the original image were explored for embedding the watermark. Watermark detection is efficient and blind in only the key and threshold but not the original image. Experimental results show that the quality of the watermarked image is good and is quite effective against general image processing and extremely robust against JPEG compression.

Keywords Watermarking, Wavelet transformation, Singular value decomposition(SVD), Singular vector quantization

1 引言

小波变换与其它变换不同,它具有独特的时频局部化特征,每个小波系数代表在确定频率范围和局部空间中的信息。低频子带中小波系数幅值非常大,聚集了图像的大部分能量,对低频系数的修改可能会造成图像明显失真。而高频子带中的小波系数代表了图像的细节信息,对低通滤波、加噪等处理非常敏感。因此现有的大部分基于小波变换的水印算法都是选取中、高频子带的系数来嵌入水印信息。黄达人[1]等通过对小波图像系数分布特点和小波系数振幅的定性定量分析,提出了把水印信息优先嵌入低频子带的水印嵌入对策和算法。

刘瑞祯等[2,3]提出了基于奇异值分解(SVD)的非盲数字水印方案,但此类算法的致命缺陷在于水印信息的提取与密钥高度相关,而与图像作品关联度较小。Zhang[4]和赵星阳等[5]对此进行了分析,指出算法的漏洞及由此引发的伪验证问题。Ahmad等[6]针对刘瑞祯等所提算法的缺陷进行改进,提出了具有不可逆性的两个水印算法,但新算法属于非盲水印方案,提取水印信息需要原始图像。Gaurav等[7]提出了基于DWT-SVD的非盲鲁棒水印算法,水印的提取需要保存从原始图像提取的低频参考图像信息,根据参考图像和水印图像提取的奇异值信息得到水印信息的奇异值,并采取与刘瑞祯等[2,3]相似的方式得到最终的灰度水印图像,水印信息与提取时提供的正交矩阵高度相关,容易实现伪验证,并不具有实用价值。

Bao和Ma[8]通过分析量化步长的统计模型,提出了自适应的DWT-SVD盲水印算法,算法对原始图像小波变换后的低频子带进行分块SVD,通过对特征值之和的量化调制来嵌入水印信息比特。算法基于低频子带中系数块的统计数属性,自适应地确定量化参数,水印提取无需原始图像。实验表明,DWT-SVD比单纯使用SVD能获得更好的性能,算法对JPEG压缩具有很强的鲁棒性,但对滤波和随机噪声比较敏感。

Chang等[9]提出一种空域分块SVD盲水印方案,算法使各图像块在经过一般图像处理操作后最大奇异值对应的奇异向量相邻系数幅值之间的关系(两相邻系数差的正负)保持一定的稳定性,以此来嵌入1bit水印信息。为了平衡水印信息的鲁棒性和不可见性,利用奇异值矩阵的非零系数个数(即它的秩)来决定该块(矩阵)的复杂度,算法选择复杂度较高的图像块来嵌入水印信息。张建伟等[10]给出了一种基于图像小

到稿日期:2010-12-28 返修日期:2011-03-23 本文受国家自然科学基金(60803136),青年科学基金项目(61004037)资助。

胡 青(1975-),女,博士生,讲师,主要研究方向为信息安全、图像数字水印,E-mail:huqing299@sohu.com;龙冬阳(1958-),男,教授,博士生导师,主要研究方向为信息安全、编码理论。

波域分块奇异值分解的自适应水印方案，即将水印嵌入到载体图像经小波低频子带分块奇异值分解后正交矩阵 U 第 1 列系数幅值的关系中，算法采用图像的局部统计特征自适应确定修改阈值，控制系数的修改幅度，力求在透明性和鲁棒性之间达到最优平衡。

Chung 等[11]论证了在水印嵌入过程中修改 U(或 V)的列矢量系数引起的视觉损坏小于修改 U(或 V)的行矢量引起的视觉损坏。Fan 等[12]通过实验对比和理论分析，提出只有 U 和 V 中的第 1 列数据对各种常规处理具有稳定性，即嵌入水印具有较强的鲁棒性。

本文在对奇异值分解及其特性进行理论探讨和实验数据分析的前提下，提出了一种新颖的奇异向量的量化嵌入策略。实验表明，本文提出的算法优于已有的基于 DWT-SVD 的水印方案。

2 奇异值分解与水印嵌入策略

奇异值分解(SVD)作为一种非常有效的数值分析技术，在图像和信号处理领域有非常广泛的应用。数值分析中的奇异值分解是一种将矩阵对角化的数值算法。从线性代数的角度来看，一幅数字图像可以看成是由一个许多非负标量组成的矩阵，如果利用矩阵的奇异分解将图像矩阵分解，就能够把图像的信息集中到奇异阵的少数奇异值及其对应的奇异向量上。给定一个 $m\times n$ 大小的实矩阵 A，其 SVD 分解可表示为：

$$A=USV^T=\sum_{i=1}^{r}\lambda_i U_i V_i^T \tag{1}$$

式中，U 和 V 分别为 $m\times m$ 及 $n\times n$ 大小的正交矩阵，$S=\mathrm{diag}(\lambda_1,\lambda_2,\cdots,\lambda_r,0,\cdots,0)$ 为非负对角矩阵，其对角元素 λ_i 即为矩阵 A 的奇异值，且满足 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_r>0$，$r$ 为 S 的秩。

SVD 的优点有：(1)SVD 分解对所要进行变换的矩阵的大小没有什么限制，可以是方阵也可以是长矩阵；(2)对于轻微的扰动和处理，图像矩阵奇异值的稳健性非常好，不会有很大的变化；(3)每个奇异值 λ_i 决定了一个 SVD 图像层的亮度(能量)，同时其对应的两个奇异向量 U_i 及 V_i^T 决定了图像的几何特征，较大的奇异值对应的奇异向量具有较强的稳定性。特别地，正交矩阵 U 的第 1 列向量(以下简记为 U_1)的两个相邻系数在经过图像处理操作后，仍能保持绝对值差的正负关系[12]。

对应 SVD 变换的优点，数据可根据需要进行任意大小规格的分块，水印信息通过不同的量化策略嵌入奇异值或相应的奇异向量中。现有的大部分基于 DWT-SVD 的算法[8,13]都是通过对小波低频或高频子带的奇异值进行量化调制来嵌入水印信息，利用奇异值的稳健性来确保水印算法的稳健性。一些基于奇异向量的关系量化嵌入方法和思路也被提出[9-11]。文献[9,10]根据嵌入的信息 bit 位的情况，在幅值差异阈值 T 的控制下对 U_1 分量相邻的两个系数幅值进行量化调制，使得幅值差大于 T 或小于 $-T$。文献[9]对一组灰度值比较平稳的图像数据进行了 JPEG 压缩，并就 U_1 分量向量系数与嵌入水印信息匹配和不匹配情况下量化调制对图像质量的影响进行了统计分析，还以 JPEG 压缩使图像像素产生的均差远大于量化调制所产生的均差，来说明嵌入水印信息后原始图像的质量不会受到很大的影响，但是如果图像块中包含明显的边缘和纹理特征，则图像块的质量将受到严重的影响。假设相邻系数阈值 T 设置为 0.002，则基于关系的量化算法必须修改矩阵 U 中的系数(例如矩阵 U 第一列第 2、3 行的系数 $U_1(2)$ 和 $U_1(3)$)来嵌入水印信息。表 1 中(a)为原始数据，(b)为 SVD 变换后的矩阵 U，其中 U_1 向量中的相邻系数 $U_1(2)$ 和 $U_1(3)$ 幅值相差较大，(c)为嵌入信息与幅值关系不匹配情况下，$U_1(2)$ 和 $U_1(3)$ 被修改为 $-0.4800(-||-0.4061|+(0.0020+0.1458)/2|)$ 和 $-0.4780(-||-0.5519|-(0.0020+0.1458)/2|)$。(d)为使用(c)重构得到的数据。对比(a)与(d)两组数据的第 2 行和第 3 行，可知此种情况下水印信息的嵌入将严重降低局部图像的质量。算法[9,10]的水印嵌入策略虽然整体上能获得较高的 PSNR，但并未考虑当对应的相邻系数幅值相差较大且与水印信息不匹配时，为嵌入水印信息大幅度修改系数必然导致原始数据局部严重失真。由此可见，利用正交矩阵 U 的 U_1 向量的两个相邻系数的幅值关系的稳定性来嵌入水印信息的算法[9,10]，不尊重相邻系数原有的相互关系，使得某些系数幅值的修改幅度没有得到很好的控制，导致算法的透明性下降。事实上单位奇异向量对应图像的几何特征，其系数值对各种攻击具有很强的稳定性，关系的稳定性是其值稳定的一种体现。直接利用最大奇异值对应的奇异向量的系数的幅值通过简单的量化来嵌入水印，可更好地控制局部失真程度，同时获得优异的稳定性。

表 1 实验数据

(a)原始数据块				(b) (a)SVD分解得到的U矩阵			
48	41	43	48	−0.2884	0.4181	0.4674	−0.7235
95	66	40	34	−0.4061	−0.5042	0.6926	0.3180
111	104	67	40	−0.5519	−0.5162	−0.5116	−0.4089
116	104	108	82	−0.6688	0.5518	−0.2000	0.4563
(c) 不匹配情况下的U阵系数修改结果[9]				(d) 使用(c)重构的数据			
−0.2884	0.4181	0.4674	−0.7235	49	41	43	48
−0.4800	−0.5042	0.6926	0.3180	109	78	50	42
−0.4780	−0.5162	−0.5116	−0.4089	97	92	57	32
−0.6688	0.5518	−0.2000	0.4563	116	104	108	82
(e) 分解(d)得到的U矩阵分量				(f) 本文保证单位性方法的修改结果			
−0.2900	0.4178	0.4930	0.3645	−0.2884	0.4181	0.4674	−0.7235
−0.4828	−0.5046	−0.5219	−0.5972	−0.4855	−0.5042	0.6926	0.3180
−0.4803	0.5167	−0.4635	0.5522	−0.4835	−0.5162	−0.5116	−0.4089
−0.6724	0.5512	0.5193	−0.4534	−0.6688	0.5518	−0.2000	0.4563
(g) (f)重构再分解得到的新的U分量							
−0.2885	0.4195	0.4435	−0.7376				
−0.4858	−0.5018	0.6515	0.2963				
−0.4833	−0.5139	−0.5570	−0.4382				
−0.6687	0.5550	−0.2620	0.4197				

奇异值变换所产生的 U 为单位正交矩阵，U_i 分量中的系数及分量之间存在一定的约束关系，如式(2)所示，$\langle|\rangle$ 表示内积运算。已有算法采取的关系量化策略并未充分考虑这一约束关系，通过对称的增减量化保证 U_1 分量包含的系数和不变，如式(3)所列，但却不能保证其内积为 1，即修改后的向量仍为单位向量。当修改的相邻系数的幅值相差较大时，此量化过程中将不可避免引入内部噪声。如表 1(e)所列，利用修改过的 U 分量(表 1(c))重构得到的数据(表 1(d))再 SVD 分解后得到的 U 矩阵的第一列系数幅值关系保持稳定，但其幅值与表 1(c)有较大的偏差。若在对 $U_1(2)$ 和 $U_1(3)$ 进行修改时注意保证 U_1 向量的单位性，即向量系数修改前后必须满足式(4)的约束，则可较好解决这一问题。如表 1(f)所列，若 $U_1(2)$ 被修改为 −0.4855，则对应的 $U_1(3)$ 则为 −0.4835，以满足修改后向量仍为单位向量($|-0.4061|^2+|-0.5519|^2=|-0.4855|^2+|-0.4835|^2$)，即式(4)的约束。如表 1(g)为

使用单位约束条件下的修改分量(表1(f))重构再分解得到的新的U分量数据,对比表1(g)与表1(f)两组数据,分量的第一列保持稳定,其它系数变化幅度也有所收窄。这里还需要注意的是,对U_1向量系数的修改必然会影响它与其它奇异向量的正交性,但由于对应的奇异值远大于其它奇异值,则重构后再分解得到的U_1向量系数值也保持了很强的稳定性,U分量的其它向量则会自适应调整,不会影响水印信息的提取。

$$\langle U_i|U_j\rangle=\begin{cases}1, & \text{if } i==j\\ 0, & \text{if } i\neq j\end{cases} \tag{2}$$

$$\sum_{i=1}^{m}|U_1(i)|=\sum_{i=1}^{m}|U_1'(i)| \tag{3}$$

$$\sum_{i=1}^{m}U_1^2(i)=\sum_{i=1}^{m}U_1'^2(i)=1 \tag{4}$$

3 向量量化水印算法

小波域中低频子带聚集了图像大部分的能量,系数幅值具有较强的稳定性。利用矩阵的奇异分解,能够把小波域的低频信息集中到奇异阵的少数奇异值及其对应的奇异向量上。对应于DWT和SVD变换的优点,本文提出一种对原始图像进行二级小波分解、对分解得到的低频子带系数进行不重叠的分块奇异值变换、对最大奇异值对应的奇异向量进行向量量化调制的水印嵌入算法,此算法相比已有算法具有更好的鲁棒性和不可见性。

3.1 奇异向量量化调制方法

较大的奇异值对应的奇异向量具有较强的稳定性,即U_1分量系数的幅值稳定性最强,为了保证算法的鲁棒性,选择U_1向量进行量化调制。须要特别注意的是,U_1向量代表了原始数据最重要的几何特性,因此量化幅度不宜过大,且对U_1向量的某个系数修改后,必须调整其它系数以满足修改后的U_1向量仍为单位向量的要求。为了嵌入水印信息比特'1'或'0',可从U_1向量包含的n个系数中任意选取一个系数,使用常用的量化方式嵌入水印信息,并根据约束条件调整其它系数。对应的量化嵌入方式如式(5)所示,T为量化阈值,w表示待嵌入的水印信息,mod为模运算,sign为取符号运算,$U_1(i),i\in[1,n]$,表示U_1向量的系数,向量大小为n,$\widetilde{U}_1(i),i\in[1,n]$表示量化后的系数。

$$\widetilde{U}_1(i)=\begin{cases}U_1(i)-\mathrm{mod}(U_1(i),T), & \text{if } w=0,\mathrm{mod}(U_1(i),T)<T/2;\text{else}\\ U_1(i)-\mathrm{mod}(U_1(i),T)+T, & \text{if } w=0,\mathrm{mod}(U_1(i),T)>T/2;\text{else}\\ U_1(i)-\mathrm{mod}(U_1(i),T)+T/2, & \text{if } w=1\end{cases}$$

$$\widetilde{U}_1(j)=sign(U_1(j))\times\sqrt{(U_1^2(i)-\widetilde{U}_1^2(i))/(n-1)+U_1^2(j)}$$

$$j\in[1,n],\text{且 } j\neq i \tag{5}$$

3.2 嵌入与提取算法

为嵌入水印信息,先对载体图像二级小波分解后的低频分量做适当大小的分块,块的大小可根据嵌入水印信息量的大小自适应调节,然后将通过量化SVD分解得到的U_1向量嵌入水印信息。为了提高算法的安全性,可对待嵌入的二值水印图像进行某种置乱操作,并可通过密钥来控制水印信息比特的嵌入位置。嵌入水印信息的具体步骤如下:

1)对载体图像进行二级小波分解,提取低频分量将其分为互不重叠的$n\times n$大小的子块。

2)根据待嵌入水印位对每一子块进行如下操作,嵌入1比特水印信息。

a. 对每个子块SVD分解得到U分量。

b. 在密钥key的控制下选择U_1向量的第i个系数在阈值T的控制下按式(5)的方法,量化嵌入1比特水印信息,并调整向量的剩余系数,以确保向量的单位性。

c. 由修改后的U分量重构子块。

3)利用嵌入水印信息的子块重组载体图像的低频分量,由逆小波变换得到嵌入水印信息的图像。

提取水印信息无需原始图像,与嵌入算法一样,对含水印信息的载体图像进行小波分解,取低频分量按嵌入算法对应的方式分块,并对每一块SVD分解得到U分量,根据嵌入密钥key和量化阈值T,选择$U_1(i)$提取嵌入的水印信息。若$|\mathrm{mod}(U_1(i),T)-T/2|<T/4$,则嵌入此块的水印信息为1,否则为0。将提取的水印信息重新排列,即得到提取的水印图像。

4 实验结果及讨论

本文以512×512的标准灰度图像"lena"、"Boat"、"Baboon"为载体图像,以32×32的二值图像为水印信息,用峰值信噪比(peak signal noise ratio,PSNR)评价原始图像与含水印图像之间的差别,并以提取出的水印图像的视觉效果和位错率(bit error ratio,BER)作为水印嵌入质量的主客观评价标准。

本文选取不同的量化阈值进行了水印信息的嵌入,并通过stirmark、photoshop和Matlab软件对含水印图像进行了各种攻击实验。实验结果表明,基于奇异向量量化的水印嵌入策略与文献[9,10]的方法相比,具有更好的透明性和鲁棒性。

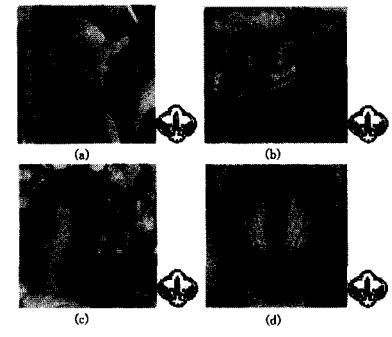

图1 载体图像及其水印信号

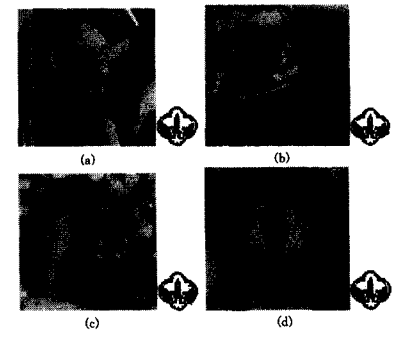

图2 含水印图像及其提取的水印

图1(a)、(b)、(c)、(d)分别是lena、boat、peppers、baboon原始图像及待嵌入的二值水印图像。图2(a)、(b)、(c)、(d)分

别是 lena、boat、peppers、baboon 用本文方法，量化阈值 $T=0.028$，$n=4$，嵌入水印后的图像（各自的 PSNR 分别为 45.3659dB、45.3426dB、45.3322dB、44.9572dB）及提取出的二值水印图像。对比原始图像和嵌入水印图像无明显视觉差别，且 PSNR 保持在 45dB 的较高水平，提取的二值水印信息与嵌入的水印信息一致。

下面以图 2(a)中嵌入水印信息的“lena”图像为例，进行算法的鲁棒性测试。

图 3 给出了水印图像经过不同质量因子的 JPEG 压缩后提取的水印信息，图 3(a)－(e)为质量因子分别为 70%、50%、30%、25%、20%（对应的 PSNR 值分别为 45.8947dB、35.9052dB、34.6264dB、33.6307dB、33.0163dB）情况下提取的二值水印图像，其对应的 BER 值分别为 0.0039、0.0176、0.0645、0.1054、0.1553。实验结果表明本文算法对 JPEG 压缩具有很好的鲁棒性，即使在 20%的质量因子下，都能较好地提取水印信息。

图 3　JPEG 压缩下提取的水印

图 4 给出水印图像经过滤波和叠加噪声处理后的实验结果。图 4(a)－(c)分别是经 3×3 的高斯滤波、中值滤波和维纳滤波（对应的 PSNR 值分别为 40.7980dB、35.5660dB、38.1857dB）后提取的水印，其对应的 BER 值分别为 0.0039、0.0371、0.0186。图 4(d)、(e)分别是水印图像经过高斯和椒盐噪声攻击（对应的 PSNR 值分别为 25.8729dB、28.3270dB）后提取的水印，其对应的 BER 分别为 0.2304 和 0.1260。实验结果表明算法对滤波攻击具有较强的鲁棒性，但抵抗噪声攻击的能力较弱，但水印信息仍可识别。

图 4　滤波和叠加噪声攻击下提取的水印

图 5 给出了水印图像经过锐化、模糊处理后的实验结果。图 5(a)、(b)分别是经过锐化、边缘锐化后（对应的 PSNR 值分别为 34.9077dB、39.8597dB）提取的水印信息，其对应的 BER 值分别为 0.0332、0.0146。图 5(c)－(e)分别是经过模糊、加强模糊和运动模糊后（对应的 PSNR 值分别为 40.8201dB、34.8551dB、25.8316dB）提取的水印信息，其对应的 BER 值分别为 0.0059、0.0459、0.1631。实验表明本算法对锐化、模糊等处理具有一定的鲁棒性。

图 5　锐化、模糊攻击下提取的水印

图 6 给出了水印图像经过扭曲和小角度旋转后提取水印的实验结果。图 6(a)－(c)分别是 ZigZag 扭曲(1,5)、波纹扭曲(50%)、旋转扭曲(5dg)后（对应的 PSNR 值分别为 30.3460dB、33.0711dB、24.8726dB）提取的水印，其对应的 BER 值分别为 0.0850、0.1387、0.1670。图 6(d)－(g)分别是含水印图像小角度旋转－0.3、－0.25、0.25、0.3 度后（对应的 PSNR 值分别为 27.8384dB、29.0661dB、29.4663dB、28.1867dB）提取的水印，其对应的 BER 值分别为 0.1494、0.1172、0.1289、0.1631。实验结果表明，本文算法对轻微的扭曲和小角度旋转等几何变换也具有一定的鲁棒性，提取的水印信息仍可识别。

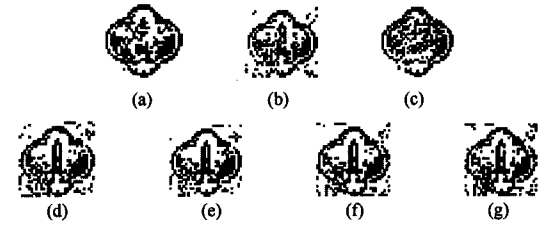

图 6　扭曲和小角度旋转攻击下提取的水印

以上给出了量化阈值 $T=0.028$ 时 Lena 含水印图像的实验结果，T 值的选取根据嵌入水印图像的质量和水印信息的鲁棒性综合决定。T 值越大，则水印信息对各种攻击的鲁棒性越强，对应的含水印图像的质量越差，反之亦然。表 2 给出了不同 T 值下（T 分别为 0.040，0.028，0.020，对应的 Lena 含水印图像的 PSNR 分别为 43.4621dB，45.3659dB，47.8277dB），提取的水印信息的 BER 对比。

表 2　不同阈值 T 下提取水印的 BER 对比

攻击 / T	JPEG 压缩(QF)			滤波(3×3)		锐化	模糊
	70	50	25	高斯	中值		
0.040	0.0000	0.0020	0.0429	0.0000	0.0088	0.0184	0.000
0.028	0.0039	0.0176	0.1054	0.0039	0.0371	0.0332	0.0146
0.020	0.0107	0.0430	0.1978	0.0195	0.0674	0.0742	0.0215

如图 1 所示，在量化阈值 $T=0.028$ 时，嵌入水印图像能获得较好的视觉效果（45dB 左右的 PSNR 值）。表 3 列出了图 1 嵌入水印信息的 baboon、peppers 和 boat 在各种攻击下，提取水印信息的 BER 值。实验结果表明对于不同的图像，使用本文提出的量化嵌入算法均能取得较好的效果。

表 3　不同测试图像提取水印的 BER 对比

攻击 / T	JPEG 压缩(QF)			滤波(3×3)		锐化	模糊
	70	50	25	高斯	中值		
Baboon	0.0019	0.0127	0.0996	0.0186	0.2090	0.1504	0.0420
Peppers	0.0189	0.0389	0.1035	0.0097	0.0459	0.0477	0.0215
Boat	0.0156	0.0332	0.0927	0.0127	0.0713	0.0713	0.0231

表 4 给出了本文提出的嵌入方案与文献[9,10]的性能比较(BER)，可见本文提出的算法在保证嵌入水印图像较高 PSNR 的前提下，具有更好的视觉效果，且对 JPEG 压缩和常规的滤波处理具有显著的优势。

表 4　不同算法提取水印的 BER 对比

攻击 / T	JPEG 压缩(QF)			滤波(3×3)		锐化	模糊
	70	50	25	高斯	中值		
本文算法	0.0039	0.0176	0.1054	0.0039	0.0371	0.0332	0.0146
文献[9]算法	0.0850	—	—	—	—	0.0001	0.0264
文献[10]算法	0.0176	0.0449	0.1611	0.0351	0.1523	0.0058	0.0527

（下转第 53 页）

但比 ANODR 及 LCAR 多，因 AnonDSR 在匿名路由请求前需要安全参数建立协议。LCAR 和 ANODR 的控制包比例相对最少。

结束语 Ad-hoc 网络节点运算能力差，能量有限且移动速度高，但已提出的匿名路由协议含有大量的公钥运算，运算量大，能量消耗大且路由建立时延长。为了降低能量消耗与路由建立时延，我们提出了一种低运算量的匿名路由协议。它将零知识证明及双线性对应用到匿名路由建立过程中，大幅降低匿名路由过程中的公钥运算量，从而降低了能量消耗和路由建立时延。

现在的双线性映射主要通过有限域上的超椭圆曲线上的 Tate 对或者 Weil 对来构造，所以下一步工作将对椭圆曲线进行研究，以提高双线性对的运算效率。

参 考 文 献

[1] Boukerche A, El-Khatib K, Xu Li, et al. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad-hoc Networks[C]// 29th Annual IEEE International Conference on Local Computer Networks(LCN'04). Tampa, Florida, USA, November, 2004

[2] Kong Jie-jun, Hong Xiao-yan, Gerla M. An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad-hoc Networks[J]. IEEE Transactions on Mobile Computing, Frequency, 2007, 6: 888-902

[3] Zhang Yan-chao, Liu Wei, Fang Yu-guang. MASK: Anonymous On-Demand Routing in Mobile Ad-hoc Networks[J]. IEEE Transactions on wireless communications, 2006, 5(9)

[4] Song Rong-gong, Korba L, Yee G. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks [C]// Proceedings of the 2005 ACM Workshop on Security of Ad-hoc and Sensor Networks. Alexandra, Virginia, USA, January 2005

[5] 许春香，李发根，聂旭云，等. 现代密码学[M]. 成都：电子科技大学出版社，2008：135-139

[6] Seys S, Preneel B. ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks[J]. International Journal of Wireless and Mobile Computing, 2009, 3: 145-155

[7] Zhu Bo, Wan Zhi-guo, Kankanhalli M S, et al. Anonymous Secure Routing in Mobile Ad-Hoc Networks[C]// Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04). Tampa, Florida, USA, November 2004

[8] Feige U, Fiat A, Shamir A. Zero Knowledge Proofs of Identity [C]// Proceedings of the nineteenth annual ACM symposium on Theory of computing. New York, USA, 1987

[9] 何德全，肖国镇，卿斯汉，等. 安全协议[M]. 北京：清华大学出版社，2005：215-217

[10] Li Xiao-qing, Li Hui, Ma Jian-feng, et al. An Efficient Anonymous Routing Protocol for Mobile Ad-hoc Networks, Information Assurance and Security 2009[C]// IAS'09. Fifth International Conference on. vol. 2, Aut. 2009: 287-290

[11] McCanne S, Floyd S. Advances in Network Simulation [EB/OL]. http://www.isi.edu/nsnam/. , July 2010

(上接第 33 页)

结束语 目前，基于 DWT-SVD 的水印方案大多都是将水印信息嵌入到奇异值中，也出现了一些利用 SVD 分解的正交矩阵第一列相邻系数关系稳定的特性来嵌入水印信息的一些算法，但这些算法通过调制相邻系数的关系来嵌入水印信息，虽然通过阈值调整来平衡算法的透明性和鲁棒性，获得了较高的 PSNR，但不可避免地会造成严重的局部失真，影响视觉效果。本文利用 SVD 分解的正交矩阵第一列系数值的稳定性，在量化阈值 T 的控制下嵌入水印信息，并根据正交矩阵向量系数间的制约关系调整其它系数值，保证嵌入信息的稳定性。实验结果表明，本文提出的算法在保证较好的透明性的前提下对各种攻击具有较强的鲁棒性，特别对 JPEG 压缩具有优异的鲁棒性，水印提取过程无须原始图像，具有极强的实用性。

参 考 文 献

[1] 黄达人，刘九芬，黄继武. 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

[2] 刘瑞祯，谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报，2001，29(2)：168-171

[3] Liu Rei-zhen, Tan Tie-niu. An SVD-based watermarking scheme for protecting rightful ownership[J]. IEEE Trans. Multimedia, 2002, 4(1): 121-128

[4] Zhang Xiao-ping, Li Kan. Comments on An SVD-Based Watermarking Scheme for Protecting Rightful Ownership[J]. IEEE Transactions on multimedia, 2005, 7(2): 593-594

[5] 赵星阳，孙继银. 一类基于奇异值分解的图像水印算法伪验证分析[J]. 计算机应用，2010，30(2)：517-520

[6] Mohammad A A, Alhaj A, Shaltaf S. An improved SVD-based watermarking scheme for protecting rightful ownership[J]. Signal Processing, 2008, 88(9): 2158-2180

[7] Bhatnagar G, Raman B. A new robust reference watermarking scheme based on DWT-SVD[J]. Computer Standards & Interfaces, 2009, 31: 1002-1013

[8] Bao P, Ma X. Image adaptive watermarking using Wavelet domain singular value decomposition[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2005, 15(1): 96-102

[9] Chang Chin-chen, Tsai P, Lin Min-hui. SVD-based digital image watermarking scheme[J]. Pattern Recognition Letters, 2005, 26 (10): 1577-1586

[10] 张建伟，鲍政，王顺凤. 图像小波域分块奇异值分解的自适应水印方案[J]. 中国图象图形学报，2007，12(5)：811-818

[11] Chung K-L, Yang Wei-ning, Huang Yong-hua, et al. On SVD-based watermarking algorithm[J]. Applied Mathematics and Computation, 2007, 188(1): 54-57

[12] Fan Ming-quan, Wang Hon-xia, Li Sheng K. Restudy on SVD-based watermarking scheme[J]. Applied Mathematics and Computation, 2008, 203(2): 926-930

[13] 黄松，张伟，陈军，等. 一个基于 DWT 的自适应数字水印算法[J]. 计算机科学，2006，33(7)：155-157