

## 基于四元数模型和奇异值分解的图像水印算法

陈善学, 冯银波\*

(重庆邮电大学 移动通信安全研究所, 重庆 400065)

(\* 通信作者电子邮箱 fengyinbo@126.com)

**摘要:** 将四元数离散余弦变换(QDCT)和奇异值分解(SVD)相结合,提出了一种在彩色图像中嵌入水印的新方法。首先,借助 Arnold 置乱对二值水印进行预处理,应用四元数理论将彩色图像进行分块 QDCT 和 SVD;然后,利用 Logistic 映射随机抽取一批图像块实现水印的嵌入。实验表明,该方法具有较强的抗 JPEG 压缩能力,对各种噪声和滤波等具有较好的鲁棒性。

**关键词:** 四元数;四元数离散余弦变换;Arnold 置乱;Logistic 映射;奇异值分解

**中图分类号:** TP391      **文献标志码:** A

## Image watermarking algorithm based on quaternion and singular value decomposition

CHEN Shanxue, FENG Yinbo\*

(Mobile Communications Security Research Laboratory, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

**Abstract:** A new method for embedding watermark in color image which combined Quaternion Discrete Cosine Transform (QDCT) and Singular Value Decomposition (SVD) was proposed. First of all, binary watermark was preprocessed with the help of the Arnold scrambling application and the color image was made block QDCT and SVD by using quaternion theory. Then, a number of image blocks were selected at random by Logistic mapping to realize the embedding of watermark. The experimental results show that this method has strong anti-JPEG compression as well as better robustness to various kinds of noise and filtering.

**Key words:** quaternion; Quaternion Discrete Cosine Transform (QDCT); Arnold scrambling; Logistic mapping; Singular Value Decomposition (SVD)

### 0 引言

所谓数字水印,即将数字、图像标志等版权信息嵌入到多媒体数据中,以起到保护版权、鉴别真伪等作用。目前,大多以静止图像为载体,水印算法都是针对灰度图像,而在日常生活中彩色图像的应用更为广泛。现有的彩色图像水印算法可大致归纳如下:1)单通道处理。通过颜色模型转换使用单色通道或者某个颜色分量信息来实现水印的嵌入。文献[1]把彩色图像 RGB 空间变换到 YCbCr 空间,然后在亮度分量中嵌入水印。文献[2]通过修改彩色图像蓝色分量值来嵌入水印。2)多通道合成。文献[3]对彩色图像的多个通道进行处理实现水印嵌入,然后将各处理结果求和。无论是单通道处理还是多通道合成,其本质都是对灰度图像的处理,因而无法很好地体现彩色图像各通道之间的相互联系。

近年来,基于四元数理论的处理技术<sup>[4-10]</sup>被逐渐熟悉并应用到彩色图像的处理中。文献[4]把水印嵌入到四元数傅里叶变换的平行分量中,含水印图像的峰值信噪比较低,抗攻击能力差;文献[5]把水印嵌入到四元数离散余弦变换后所有实部系数的中频系数中,计算量大且抗攻击能力一般;文献[6]将二值随机序列作为水印信息在四元数傅里叶变换域中嵌入,水印信息并无实际意义;文献[7]在分块的基础上进行四元数傅里叶变换和奇异值分解,将水印嵌入各块的最大奇异值;文献[8]在四元数小波变换后的中频子带的奇异值中嵌

入水印;文献[9]利用四元数奇异值分解、四元数旋转和共轭运算实现水印的嵌入和提取;文献[10]通过对彩色图像的超复数傅里叶变换,选择合适频段修改其对称系数的值来实现水印的嵌入。

英国学者 Todd 和 Sangwine 首次将四元数理论用于彩色图像的处理中。四元数将三色空间上的彩色图像描述为一个矢量整体,处理时像素各色彩通道间的光谱联系将贯穿于整个运算过程中。该数学模型已逐渐应用到彩色图像的去噪、彩色图像的压缩和编码、彩色边缘检测等多个领域。本文在研究四元数模型的基础上,将四元数离散余弦变换(Quaternion Discrete Cosine Transform, QDCT)和奇异值分解(Singular Value Decomposition, SVD)技术相结合,提出了一种基于四元数离散余弦变换和奇异值分解的彩色图像水印算法。在对彩色图像进行四元数离散余弦变换和奇异值分解的基础上,将水印信息嵌入宿主图像中。可以预见,本文算法可将水印带来的误差扩散到彩色图像的红、绿、蓝各通道,其鲁棒性和不可感知性均优于传统的单通道处理或多通道合成水印算法<sup>[11-12]</sup>。

### 1 算法的理论基础

#### 1.1 彩色图像的四元数描述

早在 1843 年英国数学家 Hamilton<sup>[13]</sup>就提出了四元数理论,直到 20 世纪 90 年代英国学者 Todd 和 Sangwine 才将四元

**收稿日期:** 2012-12-18; **修回日期:** 2013-01-16。      **基金项目:** 国家自然科学基金资助项目(61271260, 61071116, 61102062); 国家科技重大专项(2009ZX03001-004-02); 重庆市自然科学基金资助项目(CSTC2010BB2407, cstcjjA40002); 重庆市教委科学研究项目(KJ110503)。

**作者简介:** 陈善学(1966-),男,安徽合肥人,教授,博士,主要研究方向:信源编码、数字信号处理、小波分析; 冯银波(1987-),男,重庆人,硕士研究生,主要研究方向:数字图像处理、数字水印。

数理论应用到彩色图像处理领域。一个四元数可以表示为

$$q = a_0 + a_1 i + a_2 j + a_3 k \quad (1)$$

式中:  $a_0, a_1, a_2, a_3$  为实数;  $i, j, k$  为虚数单位。  $i, j, k$  之间的关系为:

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = -ji = k, jk = -kj = i, ki = -ik = j \end{cases} \quad (2)$$

从上述定义可以看出,四元数乘法不满足交换律。令四元数的实部  $a_0 = 0$ , 3 个虚部  $i, j, k$  分别代表彩色图像的红 (Red, R)、绿 (Green, G)、蓝 (Blue, B) 三个基色分量, 则彩色图像的 RGB 模型可以表示为:

$$f_q(m, n) = R(m, n)i + G(m, n)j + B(m, n)k \quad (3)$$

式中的下标  $q$  表示四元数。

### 1.2 四元数离散余弦变换及其反变换<sup>[14]</sup>

定义 1  $f_q(m, n)$  的四元数离散余弦变换 (QDCT) 可定义为:

$$QDCT_q(p, s) = \alpha(p)\alpha(s) \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \mu_q \cdot f_q(m, n) \cdot N(p, s, m, n) \quad (4)$$

式中:  $\mu_q$  是一个被称为四元数因子的单位纯四元数, 即  $\mu_q$  的模为 1, 实部为 0, 且  $\mu_q^2 = -1$ 。不同, 变换得到的结果也不同。  $f_q(m, n)$  是一个大小为  $M \times N$  的二维四元数矩阵,  $\alpha(p)$ ,  $\alpha(s)$  和  $N(p, s, m, n)$  的取值与离散余弦变换 (Discrete Cosine Transform, DCT) 类似:

$$\begin{cases} \alpha(p) = \begin{cases} \sqrt{1/M}, & p = 0 \\ \sqrt{2/M}, & p \neq 0 \end{cases} \\ \alpha(s) = \begin{cases} \sqrt{1/N}, & s = 0 \\ \sqrt{2/N}, & s \neq 0 \end{cases} \end{cases} \quad (5)$$

$$N(p, s, m, n) = \cos\left[\frac{\pi(2m+1)p}{2M}\right] \cos\left[\frac{\pi(2n+1)s}{2N}\right] \quad (6)$$

在执行四元数离散余弦变换时, 可以借助四元数矩阵的 Cayley-Dickson 形式并利用现有的离散余弦变换算法来简化计算。四元数表示为  $q = a_0 + a_1 i + a_2 j + a_3 k$ , 其 Cayley-Dickson 形式可记为  $q = A + Dj$ 。其中  $A = a_0 + a_1 i$ ,  $D = a_2 + a_3 i$ , 那么  $q = (a_0 + a_1 i) + (a_2 + a_3 i)j$ 。四元数离散余弦变换可按下述步骤进行:

1) 将  $f_q(m, n)$  表示为 Cayley-Dickson 形式  $f_q(m, n) = A(m, n) + D(m, n)j$ , 式中下标  $q$  表示四元数,  $A(m, n)$ ,  $D(m, n)$  均为复矩阵。

2) 对  $A(m, n)$ ,  $D(m, n)$  进行 DCT, 其结果可表示为  $DCT[A(m, n)]$ ,  $DCT[D(m, n)]$ 。

3) 利用步骤 2) 的结果, 构建四元数矩阵  $Q(p, s) = DCT[A(m, n)] + DCT[D(m, n)]j$ 。

4) 将步骤 3) 所得结果乘上四元数因子  $\mu_q$  获得最终的计算结果:  $QDCT_q(p, s) = \mu_q \cdot Q(p, s)$ 。

定义 2 四元数离散余弦变换对应的反变换 (Inverse Quaternion Discrete Cosine Transform, IQDCT) 可定义为:

$$IQDCT_q(m, n) = - \sum_{p=0}^{M-1} \sum_{s=0}^{N-1} \alpha(p)\alpha(s) \cdot \mu_q \cdot C(p, s) \cdot N(p, s, m, n) \quad (7)$$

式中:  $C(p, s)$  是经 QDCT 后的结果, 一个大小为  $M \times N$  的二维四元数矩阵;  $\mu_q \cdot \alpha(p)$ ,  $\alpha(s)$ ,  $N(p, s, m, n)$  的取值和 QDCT 中的定义相同。

### 1.3 图像的 Arnold 置乱

Arnold 变换是 Arnold 在遍历理论中提出的一类裁剪变换。对水印进行置乱处理, 可以增强水印信息的保密性。所谓 Arnold 置乱, 即:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (8)$$

其中:  $x, y \in \{0, 1, 2, \dots, N-1\}$  为数字图像的像素坐标, 右端  $(x, y)^T$  为输入, 左端  $(x', y')^T$  为输出,  $\pmod{N}$  为模  $N$  的运算,  $N$  一般为图像的阶数。经过置乱后的图像, 看起来杂乱无章, 而当迭代一定次数后就会恢复到原图。

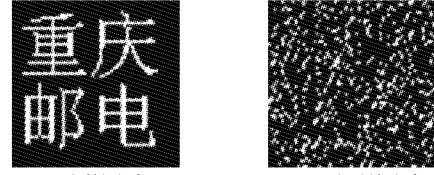


图 1 原始水印和置乱后的水印

### 1.4 图像的奇异值分解

以线性代数的角度, 一幅数字图像可以看作由许多非负标量组成的一个矩阵。图像矩阵  $I \in \mathbf{R}^{M \times N}$ , 不失一般性可表示为:

$$I = U \Sigma V^T \quad (9)$$

其中:  $U \in \mathbf{R}^{M \times M}$  和  $V \in \mathbf{R}^{N \times N}$  都是正交阵,  $\Sigma \in \mathbf{R}^{M \times N}$  是一个非对角线上的项都是 0 的矩阵, 其对角线上的元素满足:  $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r \geq \sigma_{r+1} = \dots = \sigma_M = 0$ ,  $r$  是  $I$  的秩, 它等于非零奇异值的个数。

图像的奇异值具有良好的特性: 1) 奇异值具有很好的稳定性, 不会因为较小的扰动而发生很大的变化; 2) 奇异值反映的是图像的内蕴特性而非视觉特性。

### 1.5 Logistic 映射

混沌是非线性系统中出现的确定性的、类似随机的过程。一类被广泛研究的动力系统是 Logistic 映射, 定义如下:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (10)$$

式中:  $0 \leq \mu \leq 4$ ,  $x_k \in (0, 1)$ , 这样得到的序列是单极性的, 当  $3.569945 < \mu \leq 4$  时, Logistic 映射工作于混沌状态。不同初始状态生成的序列是非周期的、不收敛、不相关的, 并对初始值非常敏感。

## 2 基于 QDCT 和 SVD 的彩色图像水印算法

由于彩色图像  $f_q(m, n)$  的实部为 0, 只包含 3 个虚部, 而频谱  $C(p, s)$  包含 4 个部分。为了保证处理后的图像仍然可以用 R、G、B 分量进行传输和显示, 要求经 IQDCT 后得到的四元数实部为 0, 否则, 图像将产生失真。经过对反变换所得结果的计算和分析, 发现其实部与  $C_r(p, s)$  无关<sup>[5]</sup>, 故选择在  $C(p, s)$  的实部系数中实现水印的嵌入。

### 2.1 水印图像的嵌入

设原始载体图像为  $f(m, n)$ , 大小为  $M \times N$ , 原始水印图像为  $W$ , 大小为  $l \times l$ , 水印的嵌入过程为:

1) 将原始水印  $W$  进行 Arnold 置乱变换 (设迭代次数为  $key$ ), 然后进行奇异值分解, 得到正交阵  $U_w$  和  $V_w$  以及对角阵  $\Sigma_w$ 。  $\Sigma_w$  的对角元素  $\sigma(i)$  ( $i = 1, 2, \dots, l$ ) 为水印图像的奇异值。

2) 将原始彩色图像载体  $f(m, n)$  分为  $k$  个互不重叠的  $8 \times 8$  子块并记为  $f^k(m, n)$ , 其中  $k = 1, 2, \dots$ ,  $round\left(\frac{M}{8} \cdot \frac{N}{8}\right)$  ( $round$  为取整函数)。设定  $\mu$  和初始状态  $x_0$ ,

得到 Logistic 混沌序列,根据  $\sigma(i)$  的长度将其处理为一个无重复元素的等长的整数序列  $T(n)$ 。根据  $T(n)$  的值,随机选取一批图像块作为水印的待嵌入区域。

3) 将选出的各待嵌入图像块  $f^k(m, n)$  用四元数形式描述并记为  $f_q^k(m, n)$ 。选取参数  $\mu_q = \frac{1}{3}(\sqrt{3}i + \sqrt{3}j + \sqrt{3}k)$ , 对每块  $f_q^k(m, n)$  执行 QDCT, 其结果记为  $C^k(p, s)$ , 并提取各实部系数, 记为  $C_r^k(p, s)$ , 其余各系数不变。

4) 计算各实部系数  $C_r^k(p, s)$  对应的 SVD, 得到正交矩阵  $U_k$  和  $V_k$  以及对角矩阵  $\Sigma_k$ , 提取各对角矩阵的最大奇异值  $\Sigma_k(1, 1)$ , 记为  $S_k(1, 1)$ 。将水印信息的奇异值  $\sigma(i) (i = 1, 2, \dots, l)$  按式(11)逐个嵌入到各对应块的最大奇异值中, 其余值不变 ( $\alpha$  为水印嵌入强度)。

$$S_{k\_new}(1, 1) = S_k(1, 1) + \alpha \cdot \sigma(i) \quad (11)$$

5) 利用公式  $C_{r\_new}^k(p, s) = U_k \Sigma_{k\_new} V_k^T$  得到嵌入水印后的实部系数。利用新的实部系数得到  $C_{new}^k(p, s)$ , 对其分别进行 IQDCT, 得到新的图像块, 记为  $f_{new}^k(m, n)$ 。

6) 将  $f_{new}^k(m, n)$  与原图像剩下的子块按原来的顺序重新组合, 得到含水印的载体图像, 记为  $f'(m, n)$ 。

## 2.2 水印图像的提取

水印信息的提取过程为:

1) 将含水印信息的图像  $f'(m, n)$  按  $8 \times 8$  分块, 通过序列  $T(n)$  选择相应的图像块并用四元数表示, 记为  $f_q^k(m, n)$ , 并按同样的方法计算各块对应的 QDCT, 记为  $C'^k(p, s)$ 。

2) 提取各实部系数, 记为  $C_r'^k(p, s)$ , 其余系数不变。将各系数进行 SVD, 按照式  $\sigma'(i) = \{S'_{k\_new}(1, 1) - S_k(1, 1)\} / \alpha$  提取各块所嵌入的水印奇异值, 再将得到的奇异值组合得到新的对角阵  $\Sigma'_{w\_new}$ , 利用公式  $W' = U_w \Sigma'_{w\_new} V_w^T$  恢复已加密水印信息, 记为  $W'$ 。

3) 根据置乱次数  $key$ , 将加密水印  $W'$  进行 Arnold 变换还原 (变换次数为  $T - key$ ,  $T$  为周期), 得到解密的水印信息, 记为  $W_{new}$ 。

## 3 实验仿真结果分析

为了定量分析提取水印与原水印的相似程度, 采用了数字水印算法中常用的归一化相关 (Normalized Correlation, NC) 系数作为评判标准。同时, 利用峰值信噪比 (Peak Signal-to-Noise Ratio, PSNR) 来度量彩色图像嵌入水印的能力, 即透明性。

本实验在 Matlab7.1 仿真软件平台下进行, 为了实验方便, 选用  $256 \times 256$  标准彩色 BMP 图像 Lena 作为原始载体, 选用有意义的  $64 \times 64$  二值图像作为水印信息。取混沌序列的初始值  $x_0 = 0.2345$ 、 $\mu = 4$ , 将得到的混沌序列通过截取、放大、取整、排序等操作后, 得到序列  $T(n) (n = 1, 2, \dots, 64)$ 。载体图像如图 2(a) 所示, 取水印嵌入强度  $\alpha = 0.1$ , 得到嵌入水印后的 Lena 图像 (图 2(c))。经计算, 其峰值信噪比  $PSNR = 47.080$ , 表明嵌入水印后的图像透明性非常好, 人眼无法直接分辨两者的差别。

为了测试本算法的抗压缩性能, 对含水印载体图像进行多次不同程度的 JPEG 压缩测试, 得到 NC 与 PSNR 值, 并与文献[5]所述算法进行对比。

由于是在 DCT 域内嵌入水印, 与图像的 JPEG 压缩标准相兼容, 可以很好地利用压缩域的特点进行水印的嵌入。如表 1 所示, 将随机选取图像块与奇异值稳定性结合起来的本

文算法抗 JPEG 压缩性能和透明性均优于文献[5]算法, 且在质量因子较低时, 也可保持强鲁棒性。



图2 嵌入效果

表1 JPEG 压缩测试

质量因子	文献[5]算法		本文算法	
	NC	PSNR/dB	NC	PSNR/dB
95	0.9612	37.446	0.9994	38.283
90	0.9450	36.475	0.9992	37.084
80	0.9390	35.345	0.9990	35.815
75	0.7973	35.090	0.9980	35.387

高斯噪声和椒盐噪声是图像传输过程中常遇干扰, 为测试本文算法对这两类噪声的鲁棒性, 对含水印载体图像进行多次实验, 分别加入不同强度的高斯随机噪声和椒盐噪声, 得到 NC 和 PSNR 值。其中, 高斯噪声的均值为 0, 方差为加入系数, 椒盐噪声的系数表示噪声密度。表 2 列出了对 Lena 图像的实验结果, 可以看出, 本文算法优于文献[5]算法, 且抗噪声攻击的性能非常好, 同时透明性也得到进一步提高。分析原因在于, 高斯随机噪声和椒盐噪声都具有随机性且嵌入的图像块为随机选取, 水印信息只嵌入部分原图像, 这在概率上以一定程度避开了噪声的影响。图像奇异值表现的是图像的内蕴特性, 具有很好的稳定性。表 3 给出了含水印载体图像经滤波和剪切后提取的水印效果。

表2 噪声测试

噪声	文献[5]算法		本文算法	
	NC	PSNR/dB	NC	PSNR/dB
高斯 0.0001	0.9644	39.270	0.9993	41.507
高斯 0.0005	0.8665	35.147	0.9995	35.726
高斯 0.001	0.7670	32.965	0.9984	33.242
椒盐 0.001	0.9270	41.532	0.9995	46.630
椒盐 0.002	0.8408	41.419	0.9993	46.226
椒盐 0.005	0.7023	41.095	0.9984	45.374
高斯 0.0001 + 椒盐 0.001	0.8903	39.258	0.9992	41.356
高斯 0.0005 + 椒盐 0.002	0.7778	35.066	0.9978	35.626

表3 滤波和剪切测试

攻击	NC	PSNR/dB
高斯低通 ( $3 \times 3$ )	0.9983	39.946
中值滤波 ( $3 \times 3$ )	0.9684	36.996
中值滤波 ( $5 \times 5$ )	0.9051	35.114
中值滤波 ( $7 \times 7$ )	0.7591	34.065
均值滤波 ( $3 \times 3$ )	0.9727	34.935
均值滤波 ( $5 \times 5$ )	0.8336	33.273
均值滤波 ( $7 \times 7$ )	0.6426	32.367
剪切 (1/16)	0.9634	35.972

可以看出, 本文算法对高斯低通滤波、中值滤波、均值滤波等常见的滤波操作具有较好的鲁棒性。由于本文算法是典型的分块算法, 不具备抗旋转攻击能力, 而对于剪切攻击, 具有一定的鲁棒性。分析原因在于, 本文算法仅随机选择一部

分图像块实现水印的嵌入,在剪切攻击下,从概率上讲一般只损失小部分水印信息,提取的水印仍能保证其有效性。

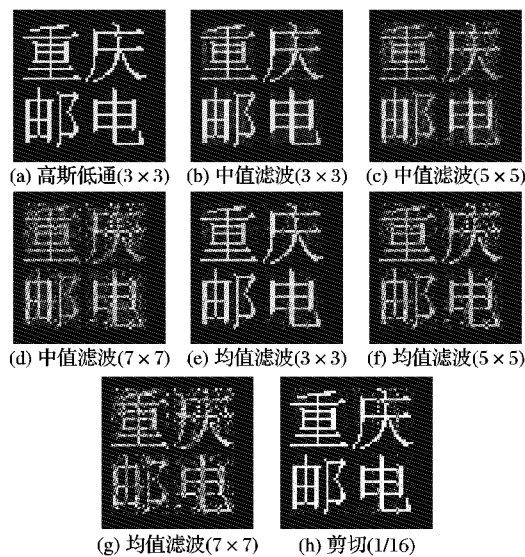


图3 滤波和剪切测试的水印信息

文献[5]通过替换各块 QDCT 后实部系数的中频系数来实现水印的嵌入,计算重复度大,且水印未经任何预处理,保密性差。直接替换中频系数,对原图像冲击比较大,必将导致 PSNR 的降低,且鲁棒性较差。从原理可知本文算法计算重复度小,同时实验结果表明,本文算法的水印保密性好且具有强鲁棒性,透明性也有所提升。

#### 4 结语

首次将四元数离散余弦变换(QDCT)和奇异值分解(SVD)相结合应用于彩色图像的数字水印算法中,提出了一种在彩色图像中嵌入水印的新方法,在四元数离散余弦域中的实部系数奇异值中实现水印的嵌入。在嵌入时,将 Arnold 置乱后的水印奇异值按顺序逐个嵌入随机选取图像块的最大奇异值中。本文将四元数模型处理的优势与奇异值的稳定性结合起来,实验表明:该算法对常见的噪声、JPEG 压缩及各种滤波具有较强的鲁棒性。四元数模型在彩色图像领域的应用

处于初级阶段,还有大量的工作需要完成,本文为四元数在彩色图像水印方面的应用做了很好的补充,也为彩色图像的版权保护提供了一种新方法。

#### 参考文献:

- [1] 凌贺飞,卢正鼎,杨双远.基于 YCbCr 颜色空间的二维 DCT 彩色图像数字水印实用技术[J].小型微型计算机系统,2005,26(3):482-484.
- [2] KUTTER M, JORDAN F, BOSSEN F. Digital signature of color images using amplitude modulation[C]// Proceedings of SPIE Electronic Imaging, Storage and Retrieval for Image and Video Databases V. [s. l.]: SPIE, 1997: 518-526.
- [3] 李晓强,薛向阳.基于多通道的彩色图像水印方案[J].计算机学报,2004,27(9):1238-1244.
- [4] BAS P, BIHAN N L E, CHASSERY J M. Color image watermarking using quaternion Fourier transform[C]// IEEE International Conference on Acoustics, Speech, and Signal Processing. Piscataway: IEEE, 2003: 521-524.
- [5] 盖琦,孙云峰,王晓雷,等.基于离散四元数余弦变换的彩色图像数字水印技术[J].光电子·激光,2009,20(9):1193-1197.
- [6] 孙菁,杨静宇,傅德胜.彩色图像四元数频域幅值调制水印算法[J].计算机科学,2011,38(3):123-126.
- [7] 孙菁,杨静宇,傅德胜.彩色图像四元数频域奇异值分解水印算法[J].信息与控制,2011,40(6):813-818.
- [8] 殷明.基于四元数小波变换和奇异值分解的图像水印[J].合肥工业大学学报:自然科学版,2011,34(12):1913-1916.
- [9] 李岩山.一种新的彩色图像盲水印算法[J].计算机应用研究,2011,28(1):349-351.
- [10] 江淑红,张建秋,胡波.一种超复数频域的有意义数字水印算法[J].系统工程与电子技术,2009,31(9):2242-2248.
- [11] 李红丽,赖慧成.基于哈达玛变换和奇异值分解的四个彩色图像水印算法[J].计算机应用,2010,30(11):3025-3027.
- [12] HUANG F J, GUAN Z H. A hybrid SVD-DCT watermarking method based on LPSNR[J]. Pattern Recognition Letters, 2004, 25(15): 1769-1775.
- [13] HAMILTON W R. Elements of quaternions[M]. London: Longmans, Green, and Co, 1866: 129-133.
- [14] FENG W, HU B. Quaternion discrete cosine transform and its application in color template matching[C]// Congress on Image and Signal Processing. Washington, DC: IEEE Computer Society, 2008: 252-256.

(上接第 1621 页)

信节点私钥不泄露的情况下,协议满足 plausible routing。

此外,本方案包含了一个对  $TS_i$  的出测试,出测试的新鲜性质保证了协议中  $TS_i$  的新鲜性,可以防止恶意的重放攻击。

#### 4 结语

本文首先介绍了 LAOR 协议,随后分析其面临的安全威胁,并针对可能的安全威胁进行安全改进。分析表明改进的协议可以保证路由控制分组的完整性、新鲜性,并且可以实现节点间的相互认证,满足 plausible routing,是安全的。ACK 机制可以根据节点的反馈,发现丢包攻击。本文的改进在卫星网络中具有一定的应用价值。

#### 参考文献:

- [1] 李喆,刘军.卫星网络安全路由研究[J].通信学报,2006,27(8):113-118.
- [2] 郝选文,马建峰,任方.空间信息网络环境下一种基于双层卫星网络的认证路由协议[J].计算机科学,2011,38(2):79-81.
- [3] KARAPANTAZIS S, PAPAPETROU E, PAVLIDOU F N. On-demand routing in LEO satellite systems[J]. Computer Networks, 2007, 51(15):4356-4376.

- [4] 王汝传,饶元,郑彦,等.卫星通信网路由技术及其模拟[M].北京:人民邮电出版社,2010.
- [5] 王梅,吴蒙. MANET 网络中常见的路由安全威胁及相应解决方案[J].通信学报,2005,26(5):106-112.
- [6] AWERBUCH B, HOLMER D, NITAROTARU C. An on-demand secure routing protocol resilient to byzantine failures[C]// Proceedings of the 1st ACM Workshop on Wireless Security. New York: ACM, 2002: 21-30.
- [7] 罗长远,李伟,刑洪智,等.空间中基于身份的分布式密钥管理研究[J].电子与信息学报,2010,32(1):183-188.
- [8] GERGELY A C S, LLEVENTE B, ISTVAN V. Provably secure on-demand source routing in mobile Ad Hoc networks[J]. IEEE Transactions on Mobile Computing, 2006, 5(11):1533-1546.
- [9] 毛立强,马建峰,李兴华.可证明安全的 Ad Hoc 按需路由协议分析[J].通信学报,2009,30(1):38-44.
- [10] 季晓君,田畅,张毓森. MANET 路由协议安全分析[J].应用科学学报,2007,25(1):30-34.
- [11] 闫丽丽,彭代渊. Ad Hoc 网络中 ARAN 路由协议的安全性分析[J].电子与信息学报,2010,32(9):2241-2244.
- [12] 刘家芬.安全协议形式化分析中认证测试方法的研究[D].成都:电子科技大学,2008.