

一种有关 DWT 与 SVD 相结合的 多功能水印新方案

杨 智,王运琼,冯乔生,罗 可,冉 婕,章秀君

(云南师范大学 计算机科学与技术学院,云南 昆明 650092)

摘 要:提出了基于 DWT 和 SVD 相结合的多功能数字水印算法,主要用于图像版权保护和图像认证。该算法选取奇异值量化的方法分别嵌入鲁棒性水印和脆弱水印,鲁棒性水印主要用于适用于图像版权保护,脆弱水印主要用于检测图像被篡改的位置。在该方案中,采用分块双重置乱技术用于水印图像隐藏的预处理,以保障水印的安全性。实验结果表明,该算法不仅对 JPEG 有损压缩、中值滤波、剪切、低通滤波等各种图像降级处理有很强的稳健性,同时对图像篡改位置进行精确的检测,以抵抗抗擦除或伪造易损水印的攻击。

关键词:DWT;SVD;置乱技术;鲁棒水印;脆弱水印

中图分类号:TP391

文献标识码:A

文章编号:1673-629X(2010)07-0140-05

New Multi-function Watermark Scheme Based on DWT and SVD

YANG Zhi, WANG Yun-qiong, FENG Qiao-sheng, LUO Ke, RAN Jie, ZHANG Xiu-jun

(School of Computer Science and Information Technology, Yunnan Normal University,

Kunming 650092, China)

Abstract: Proposes a multi-function digital watermark algorithm based on Discrete Wavelet Transformation(DWT) and Singular Value Decomposition(SVD), which is mainly used for image copyright protection and authentication. A new algorithm with the method of embedding the robust watermark and fragile watermark into the singular value is proposed. Robust watermarking is mainly used for image copyright protection, fragile watermarking is mainly used for detecting location of the image which has been tampered. In the scheme, Duple scrambling technology is used as pre-processing watermarking image information hiding, so that safeguarded the watermark security. Experiments and attack testing show that the algorithm is strongly robust to different types of attacks such as JPEG compression, median filter, cropping, Gaussian low-pass filtering and so on. At the same time it can indicate the locations that have been modified, so that can robust to erase or forge fragile watermark.

Key words: DWT;SVD;rambling technology;robust watermark;fragile watermark

0 引 言

随着网络技术的高速发展,大量个人信息在网络上传播。信息的安全性成了人们关注的热点,而信息安全中图像安全是大家所关心的。数字水印技术是近年来出现的一种有效的版权保护技术,可用来标识产品所有者、进行作品认证、跟踪产品的传播及进行安全控制等。它可作为一种数据认证和版权保护的手段。

因此,信息安全研究领域中最热门的技术非数字水印技术莫属。

由于实际应用的要求不同,数字水印可以分为鲁棒性水印、脆弱性水印和半脆弱性水印。鲁棒水印要求能够抵抗各种破坏水印的攻击,适用于版权保护;如果图像有任何改变(哪怕是一个像素的改变),嵌入的水印都将被破坏,这就是脆弱水印,它能用于体现内容保护和真实性、完整性认证;由于半脆弱水印主要介于鲁棒水印和脆弱水印中间,它既可以对改变图像感知内容的任何操作保持高度敏感,也可以对不改变图像感知内容的操作具有一定的抵抗能力,尤其是 JPEG 压缩^[1,2]。有的文献把脆弱水印称为精确认证,把半脆弱水印称为模糊认证。

收稿日期:2009-11-07;修回日期:2010-02-13

基金项目:云南省科技计划科研基金资助项目(07Z40092)

作者简介:杨 智(1983-),男,湖北武汉人,硕士研究生,研究方向为图像处理与模式识别;王运琼,博士,教授,研究方向为图像处理、模式识别和智能交通;冯乔生,教授,研究方向为虚拟现实技术和计算机视觉。

多功能数字水印^[3]是指在同一数字产品中嵌入不同性质的水印,达到不同的目的。图像多功能水印可以看成是在图像中同时嵌入一个脆弱水印和一个鲁棒水印,前者用于篡改提示,后者用于版权保护。2008 年 Lee 等人^[4]提出了一种用于图像篡改检测和恢复的双水印算法,该算法将一个图像块的水印信息分别嵌入在两个不同的图像块中,当一个水印信息丢失时,还可以利用另一个水印信息恢复篡改块,从而大大提高了可恢复水印算法的篡改恢复质量。文中提出了一种 SVD 和 DWT 相结合的多功能水印算法,主要先从 DWT 域选取出合适水印嵌入的子带图像,再对其进行分块,并对子块进行 SVD 分解,修改其左矩阵 U 和右矩阵 V 的相关系数来实现水印嵌入和提取。因为 DWT 域比空间域更好于嵌入水印,而且不影响载体图像的质量。由于基于 SVD 变换水印的嵌入对图像滤波、图像增强、图像锐化和图像压缩具有很好的鲁棒性,因此文中提出的算法是将二者的优点结合起来,既保证了对内容篡改保持最大敏感度,又保证对不改变内容的有损压缩等攻击具有很强的鲁棒性。实验结果表明,该算法在篡改定位和篡改检测等方面都具有较好的性能。

1 理论依据

1.1 小波变换(DWT)

小波变换^[5,6]已经广泛地应用于数字信号处理领域,尤其在图像处理方面的成就最为显著。由于离散小波转换在处理静态图像信号时具有高度的弹性,并且能够适应人类的视觉反应,因此最近几年常被应用于图像信号上。小波变换在时间-空间域上都提供了多解析度多频率的特性。而这是静态图像与动态图像在编码应用时不可或缺的特性。小波变换是先对图像进行水平滤波再对垂直方向滤波,最后可以得到四个频带子图,如此反复,可对数字图像进行多级小波分解(如图 1 所示)。通过实验结果发现,在三级小波分解的子图嵌入水印能提高鲁棒性,但嵌入水印后的图像会产生明显失真,影响图像质量。而一级小波分解虽然满足不可感知性的要求,但会使鲁棒性下降,故使用两级小波分解既能够很好地满足不可感知性的要求,同时能满足水印的鲁棒性。

1.2 矩阵的奇异值分解(SVD)

从图像处理的角度来看,奇异值分解^[7~9]具有以下主要特性:图像的奇异值具有很高的稳定特性,即便图像受到轻微的篡改时,图像的奇异值并不随着图像的变化而剧烈的改变,可以得出矩阵的奇异值能够表现出图像内在的代数特性。

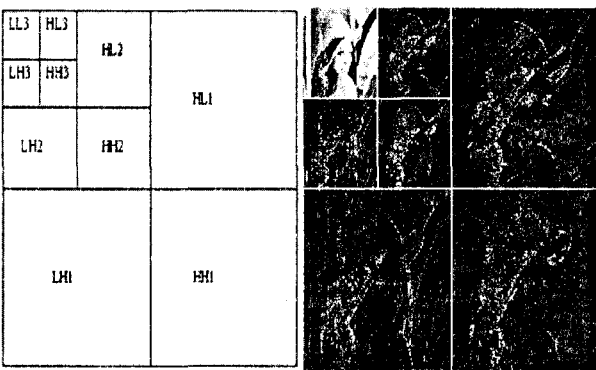


图 1 二维图像小波分解示意图

SVD 分解本身是线性代数的一种工具,但是,随着将这种特性引入到图像处理的各个方面,引起了广泛的关注。SVD 分解原理如下:大小为 $m \times n$ 的矩阵 $A \in C^{m \times n}$ 的奇异值分解为:

$$A = UDV^T = \sum_{i=1}^r \lambda_i u_i v_i^T \tag{1}$$

其中 $U \in C^{m \times n}$, $V \in C^{m \times n}$ 是 2 个酉矩阵,即 $U^T U = E$, $V^T V = E$ 。 D 表示元素为非负数的对角阵, $r \leq \min\{m, n\}$ 是矩阵 A 的秩,其中, $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n \geq 0$, 这里 σ_i 被称为 A 的奇异值, u_i, v_i 分别对应着奇异值 σ_i 的左右奇异向量,且满足以下等式:

$$A v_i = \sigma_i u_i \quad A u_i = \sigma_i v_i \quad (i = 1, 2, \dots, r) \tag{2}$$

因此 U 和 V 的列分别是 AA^T 和 $A^T A$ 的特征向量,式 (1) 便称为 A 的奇异值分解(SVD) 式。

1.3 新型变换矩阵 W

新型变换矩阵 W ^[4] 与 Arnold 矩阵^[11,12] 类似,但是,在同阶情况下,前者比后者的周期长(如表 1 所示),因为,周期越长,安全性就越强。所以,新型变换矩阵 W 在图像置乱应用中更加有优势。文中用到二阶新型变换矩阵 W 。根据数字图像处理的需要,图像置乱的 W 变换可以改写为:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \tag{3}$$

其中 $x, y \in (0, 1, 2, \dots, N - 1)$, 代表图像中像素点的坐标位置,而 N 代表矩阵的阶数。

表 1 二阶 W-矩阵和 Arnold 矩阵周期对比

N	8	16	32	64
W 矩阵周期	12	24	48	96
Arnold 矩阵周期	6	12	24	48
N	128	200	256	512
W 矩阵周期	192	60	384	768
Arnold 矩阵周期	96	150	192	384

一般来讲, W -矩阵变换的周期都比 Arnold 矩阵变换的周期要大,这样就增强了非法破解的难度。文中

提出基于块置乱,先对水印图像进行分块置乱,再对图像子块置乱。这种双重置乱方法可以大大提高算法的速度和破解的难度。

2 算法

2.1 水印嵌入算法

在文中,载体图像以大小 512×512 的灰度图像 I 、一个待嵌入的二值鲁棒水印图像大小为 32×32 的图像 W_1 ,另一个待嵌入的二值脆弱水印图像大小为 128×128 的图像 W_2 作为实验数据,以下为具体的水印嵌入算法。

2.1.1 鲁棒水印的嵌入

步骤1) 对原始水印 W_1 进行分块置乱,再对每个小子块进行置乱,通过双重置乱得到待嵌入的水印 W_2 ,将两次置乱的密钥 key_1 和 key_2 保存起来;

步骤2) 对原始灰度载体图像 I 进行二级离散小波变换(DWT),选取低频子带 LL_2 (如图1所示),对低频子带 LL_2 按照 8×8 进行分块,对每块进行置乱,再对其进行奇异值变换。比较子块中左矩阵 U 中第一列的第三行系数值和第四行系数值的大小关系来嵌入水印。判断如下:

当待嵌入的水印比特值为1时,必须保证 $|u_{31}| - |u_{41}| \geq T$ (T 是阈值)成立,如果不成立,修改系数 u_{31} 和 u_{41} 的值来保证上述成立。

当待嵌入的水印比特值为0时,必须保证 $|u_{41}| - |u_{31}| \geq T$ 成立,如果不成立,修改系数 u_{41} 和 u_{31} 的值来保证上述成立。

步骤3) 对每块进行反置乱,再进行奇异值反变换,得到新的 LL_2' 子带,再通过离散小波反变换得到新的含鲁棒水印的图像 I' 。

2.1.2 脆弱水印的嵌入

步骤1) 对含鲁棒水印图像 I' 进行分块;

步骤2) 对每个子块进行SVD分解,根据脆弱水印 W_2 嵌入水印。通过判断子块右矩阵 V 第一行的第三列和第四列系数值来嵌入水印。判断如下:

如果嵌入的水印比特为1时,必须保证 $|v_{13}| - |v_{14}| \geq T$ (T 是阈值)成立,如果成立,系数 v_{13} 和 v_{14} 值不变。如果不成立,修改系数 v_{13} 和 v_{14} 的值来满足不等式成立。

如果嵌入的水印比特值为0时,必须保证 $|v_{14}| - |v_{13}| \geq T$ 成立,如果成立,系数 v_{14} 和 v_{13} 不变。如果不成立,修改系数 v_{14} 和 v_{13} 的值来满足不等式成立。

步骤3) 对每子块进行反置乱,再对其进行奇异值反变换,得到新的含脆弱水印的图像 I'' 。

2.2 数字水印提取算法和检测算法

以下为数字水印的提取算法的描述过程。

2.2.1 鲁棒水印的提取

步骤1) 对待测试图像 I''' 进行离散小波变换(DWT),选取 LL_2 子带,再按照 8×8 分块,然后对每个子块置乱再进行SVD变换;

步骤2) 判断,如果 $|u_{31}| - |u_{41}| \geq 0$,则提取水印的比特为1,否则为0;

步骤3) 根据密钥 key_1, key_2 通过 W -矩阵反变换得到二值水印。

2.2.2 脆弱水印的提取

步骤1) 对待测试图像 I''' 进行分块,再对每个子块进行SVD分解;

步骤2) 判断,如果 $|v_{13}| - |v_{14}| \geq 0$,则提取水印的比特为1,否则为0;

步骤3) 最后得到二值水印。

2.2.3 篡改图像定位

步骤1) 先对水印图像 I 和被篡改图像 I''' 进行分块;

步骤2) 比较两者子块是否相似,如果相似,则将前者子块全部数值置1;否则将前者子块全部数值置0;

步骤3) 输出图像,可以辨别篡改的位置。

3 实验结果及分析

文中采用MathWorks公司开发的Matlab7.6版本作为仿真实验环境。所用的载体图像为常用的标准灰度图像 512×512 的“Lena”,如图2(a)所示,而嵌入的水印是大小 32×32 的二值鲁棒水印图像,如图2(b)所示,和 128×128 的二值脆弱水印图像,如图2(c)所示。然后根据所提出的水印嵌入算法和提取算法进行实验分析。由于阈值的大小影响修改图像的强度和水印图像提取的清晰程度,所以,为了慎重考虑,通过不同数据进行实验,选取阈值为0.01可以满足上面两个方面。

文中引用含水印图像和原宿主图像的峰值信噪比(PSNR)和均方差(MSE)来定量地描述算法的不易察觉性,PSNR越大,MSE越小,不易察觉性越高。引用提取的水印信息与嵌入的水印信息之间的归一化互相关系数(NC)来客观定量描述算法的鲁棒性,NC越大,鲁棒性越强。

与原始图像对比,如图2(d)所示,在视觉上已经嵌入水印图像与原始图像根本没什么根本区别,且它的峰值信比(PSNR)的值为39.4209dB,提取水印的归一化相关系数(NC)为1,可见该算法的透明性和水印

识别性都比较好。

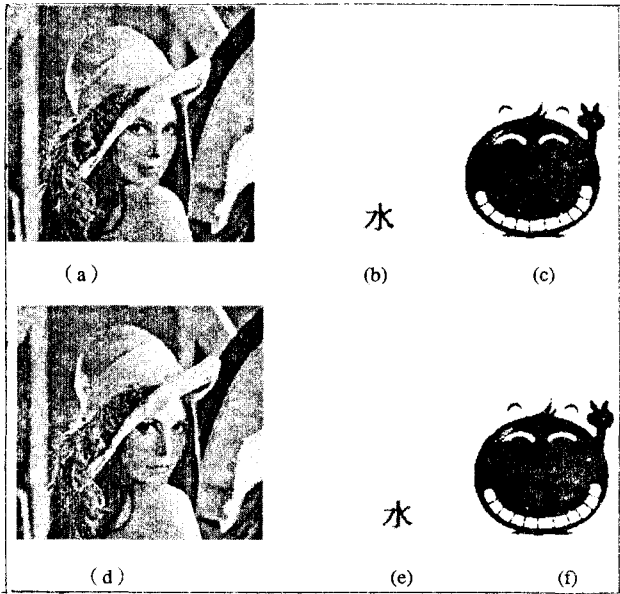


图 2 实验数据图

图 2 中,(a)原始图像;(b)鲁棒性水印;(c)脆弱性水印;(d)双水印图像;(e)未被攻击时提取的鲁棒水印;(f)未被攻击时提取的脆弱水印。

为了验证该算法对一般攻击的抵抗性,文中选取比较常用的攻击方式,例如:剪切攻击、中值过滤攻击、加入椒盐噪声攻击、JPEG 压缩攻击等等,然后用所提出的水印提取算法进行水印的提取和检测,所得实验结果如图 3 所示。

从表 2 的实验结果可以得出以下结论,该水印算法对任意剪切攻击和 JPEG 有损压缩有很好的抵御能力,并且对各类滤波攻击、各种类型的噪声攻击也具有较好的鲁棒性,但是对任意旋转攻击的提取出的水印效果不理想。

为了检测算法对图像篡改的定位能力,将嵌入水印后的图像进行局部的篡改。具体方法是将图像进行剪切和替换处理,对篡改图像进行水印提取,并和原始水印进行比较,如图 4 所示,图中白色代表差别。实验表明,算法对图像的篡改具有较好的定位能力。

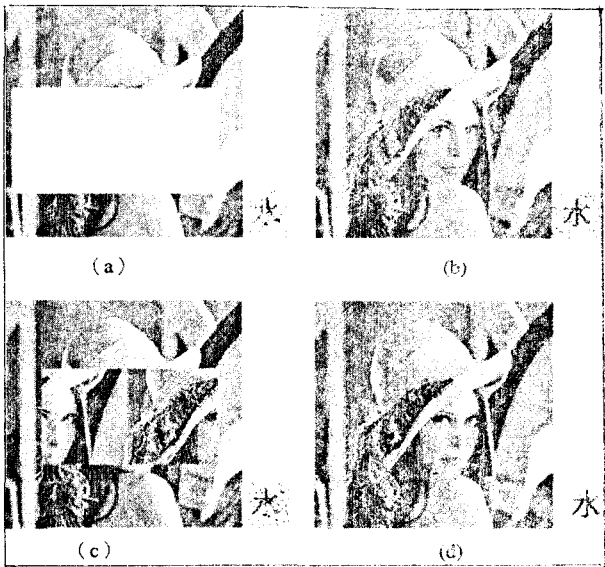


图 3 图像攻击与提取实验结果

图 3 中,(a)剪切攻击;(b)噪声攻击;(c)拼凑攻击;(d)压缩攻击。

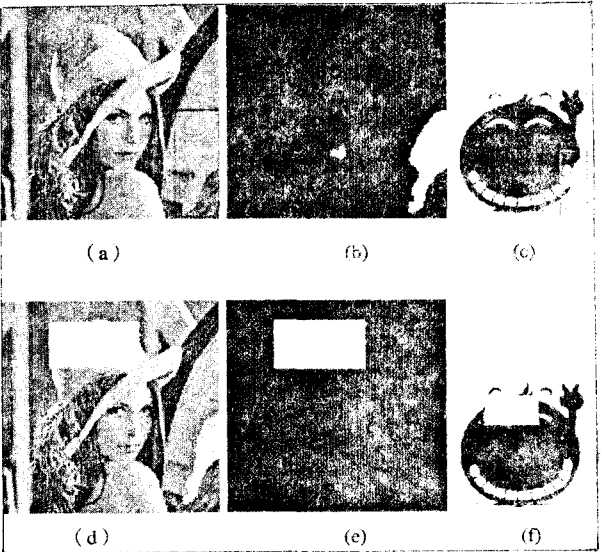


图 4 篡改检测定位实验

图 4 中,(a)待认证图像;(b)篡改定位图;(c)提取脆弱水印;(d)待认证图像;(e)篡改定位图;(f)提取脆弱水印。

表 2 几种不同攻击后提取的水印与原鲁棒水印的相似度

攻击方式	图 3(d) 未受攻击	图 3(a) 1/2 剪切	图 3(b) 加椒盐噪声	图 3(c) 拼凑	图 3(d)JPEG 压缩 (Q=90%)
NC	1	0.9921	0.9028	0.8034	0.9842
攻击方式	JPEG 压缩 (Q=80%)	JPEG 压缩 (Q=70%)	JPEG 压缩 (Q=60%)	高斯滤波(3×3)	旋转 (30 度)
NC	0.9322	0.8633	0.7661	0.8893	0.6927

4 结束语

文中提出了一种基于 DWT 与 SVD 相结合的多功能水印新方案,该方案利用 DWT 特性和 SVD 分解的稳定性,并保持了载体图像的不可视性和鲁棒性的均衡性。通过实验结果和攻击测试得出,该算法能够对剪切攻击、JPEG 压缩攻击、噪声攻击、拼凑攻击等图像处理具有很好的抵御能力,尤其是对剪切、JPEG 压缩等攻击。同时,能有效检测图像恶意攻击和进行篡改定位。但此方法在任意旋转攻击提取出的水印不够理想,希望在将来的工作中进一步的改进。总的来说,本算法在检测过程中不需要原始水印和原始图像,可以克服载体媒体占用空间过大的缺点,此外嵌入和提取算法简单,运行速度比较快速,可以说一种比较理想的数字水印方案。

参考文献:

- [1] Cao J G, Fowler J E, Younan N H. An Image - Adaptive Watermark Based on a Redundant Wavelet Transform [C]//in Proceedings of the International Conference on Image Processing. Thessaloniki, Greece: IEEE, 2001: 277 - 280.
- [2] Kourkchi H, Ghaemmaghami S. Image Adaptive Semi - fragile Watermarking Scheme Based on RDWT - SVD [C]//in proceeding of the 5th international conference in innovations in in-

formation technology. United Arab Emirates: [s. n.], 2008.

- [3] 于帅珍,沈建国.基于小波域的自适应彩色图像双重水印算法[J].微计算机信息,2006,22(1):190 - 192.
- [4] Lee T Y, Lin S D. Dual Watermark for Image Tamper Detection and Recovery [J]. Pattern Recognition, 2008, 41: 3497 - 3506.
- [5] Ho Seok Moon, Myung Ho Sohn, Dong Sik Jang. DWT-based image watermarking for copyright protection [J]. Artificial Intelligence and Simulation, 2004(3397): 490 - 497.
- [6] 李养胜,李俊.基于小波分解的图像数字水印算法[J].计算机技术与发展,2008,18(12):150 - 152.
- [7] 马建湖,何甲兴.基于小波变换的零水印算法[J].中国图象图形学报,2007,12(4):581 - 585.
- [8] Chang Chin - Chen, Tsai Piyu, Lin Chia - Chen. SVD - based digital image watermarking scheme [J]. Pattern Recognition Letters, 2005, 10(26): 1577 - 1586.
- [9] 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.
- [10] 吴亚丽.置乱的新型 W 变换矩阵[J].电子科技,2008,21(3):69 - 72.
- [11] 许红山.置乱技术在信息隐藏中的应用[J].广州大学学报,2004,3(2):134 - 136.
- [12] 董梅,高康.矩阵奇异值分解和 Arnold 置乱技术在图像隐藏中的应用[J].山东大学学报:理学版,2005,40(3):71 - 75.

(上接第 139 页)

6 结束语

通过对颜色值进行编码,使用一个值表示多种颜色,从而减少了存储状态所需要的空间,同时因为表示状态所需要的变量减少,在进行状态转移的时候赋值次数减少,赋值所需要的时间也显著减少。在空间和性能方面都有提高。但是文中采用的方法也存在一个缺点:因为采用一个值表示多个元素,修改某个具体元素需要多步操作。所以当状态中包含的元素比较多,而元素的种类比较少,并且状态转移所需要修改的元素比较少的时候,文中提出的方法具有显著的优势^[11,12]。

参考文献:

- [1] 王永庆.人工智能原理与方法[M].西安:西安交通大学出版社,1998.
- [2] 刘志镜,王小愚,李绪成,等.一种新的项集表示方法[J].计算机工程与设计,2002,23(6):42 - 44.
- [3] 许精明.状态空间的启发式搜索方法研究[J].微机发展(现更名:计算机技术与发展),2002,12(4):87 - 79.
- [4] 满君丰,刘强,杨鼎.空间数据的表示方法研究[J].计

算机应用,2004(11):97 - 99.

- [5] 徐宝祥,叶培华.知识表示的方法研究[J].情报科学,2007(5):690 - 694.
- [6] 年志刚,梁式,麻芳兰,等.知识表示方法研究与应用[J].计算机应用研究,2007(5):234 - 236.
- [7] 陈华竣,郑智,倪德明.真前缀标记树——一种面向用户的子树选取策略表示方法[J].计算机技术与发展,2006,16(12):9 - 12.
- [8] Pelegri A, Shan Baoxiang. Dynamic analysis of soft tissues using a state space model [R]. US: American Society of Mechanical Engineers (ASME), 2008.
- [9] Berners - Lee T, Hendler J, Lassila O. The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities [J]. Scientific American, 2001, 13(5): 100 - 105.
- [10] 汤赛丽,郑逢斌.基于问题的面向对象知识表示方法的研究[J].现代计算机,2005(8):13 - 15.
- [11] Tao JunYuan, Li DeSheng. Cooperative strategy learning in multi - agent environment with continuous state space [C]// 2006 International Conference on Machine Learning and Cybernetics. [s. l.]: [s. n.], 2006.
- [12] Zhang Chengjin, Bitmead B R. MIMO Equalization With State - Space Channel Models [J]. IEEE Transactions on Signal Processing, 2008, 56(10): 5222 - 5231.