# 基于 Logistic 混沌映射的 DCT 域脆弱数字水印算法

李赵红, 侯建军
(北京交通大学电子信息工程学院, 北京 100044)

摘 要: 本文提出了一种新的混沌脆弱数字水印算法. 利用混沌系统对初值的极端敏感性和块不相关水印技术, 将图像 DCT 次高频系数和水印密钥合成为 logistic 混沌映射初值从而生成水印, 再将水印嵌入到图像 DCT 的高频系数中得到水印图像. 利用图像 DCT 系数之间的关系, 实现了水印的盲检测. 实验结果表明, 该算法可以精确检测到对水印图像的一个像数点的改变, 并具有良好的定位篡改能力.

关键词: 脆弱数字水印; 混沌; Logistic 映射; 图像认证
中图分类号: TN919, TP391 文献标识码: A 文章编号: 0372-2112 (2006) 12-2134-04

# DCT-Domain Fragile Watermarking Algorithm Based on Logistic Maps

LI Zhao-hong, HOU Jian-jun
(*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China*)

**Abstract:** A new chaotic fragile watermarking algorithm is presented. With the high sensitivity on initial value of the chaotic mapping and the block-wise independent technology, the image DCT sub-high coefficients and a watermarking key are combined as the initial value of logistic maps for the generation of the watermarks, then the watermarks are embedded into the DCT high coefficients to get watermarked image. The watermarks can be blindly extracted according to the DCT coefficients. Experimental results show that the algorithm can detect any modification to the watermarked image and localize the tampers on the watermarked image.

**Key words:** fragile watermarks; chaos; logistic maps; image authentication

## 1 引言

随着计算机网络和通信技术的飞速发展, 数字媒体(包括数字图像、数字视频、数字音频)已得到了广泛的应用, 随之而来的数字媒体的信息安全、知识产权保护和认证等问题也变得日益突出. 传统的加密系统在数据传输过程中可以起到保护作用, 但数据一旦被接收并解密, 其保护作用也随之消失, 数字水印作为传统加密方法的有效补充手段, 是一种可以在开放的网络环境下保护版权和认证来源及完整性的技术, 近年来已引起了人们的高度重视[1~6]. 脆弱水印特别适用于数字产品的认证, 内容篡改的证明和完整性证明. 由于混沌系统对初值的极度敏感性, 把混沌应用到数字水印技术的研究也受到了越来越多研究者的关注[1~5], 其中大部分仅仅应用混沌系统对生成水印进行加密, 也就是传统的混沌加密技术[3~5]. 一部分研究利用混沌映射生成了与图像特征有关的水印[1]或密钥[2].

本文在对已有混沌数字水印技术的分析基础上, 提出了一种新的混沌脆弱数字水印算法. 利用混沌系统对初值的极端敏感性, 并结合块不相关技术, 提出了与图像的 DCT 系数紧密相关的水印生成和嵌入算法. 该算法具有脆弱水印的四个重要特性: (1) 不可见性; (2) 对水印图像的篡改敏感性; (3) 篡改定位能力; (4) 盲检测, 即提取水印不需要原始图像.

## 2 Logistic 映射和块不相关水印技术

### 2.1 Logistic 映射

混沌现象是在非线性动态系统中出现的确定性、类随机的过程, 这种过程非周期、不收敛但有界, 并且对初始值有极其敏感的依赖性. 利用这一性质, 混沌映射可提供数量众多、非相关、类随机而又确定, 易于产生和再生的信号.

Logistic 映射是一类非常简单却被广泛研究的混沌动力系统, 可用非线性差分方程来描述:

$$x_{n+1}=\lambda x_n(1-x_n),\quad \lambda\in[0,4],\ x_n\in[0,1] \tag{1}$$

研究发现, logistic 映射的混沌区域为 $\lambda\in[\lambda_\infty,4]$, $\lambda_\infty=3.569945672\cdots$. 理论上已经证明了由两个不同初值 $x_0$ 和 $y_0$ 生成的两个混沌序列 $x_0, x_1, \cdots, x_n$ 和 $y_0, y_1, \cdots, y_n$ 的互相关为零, 这体现了 logistic 混沌映射对初值的极度敏感性.

当 $\lambda=4$ 时, logistic 混沌序列的概率分布密度函数为:

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}}, & x\in(0,1)\\ 0, & \text{其他}\end{cases} \tag{2}$$

收稿日期: 2005-11-09; 修回日期: 2006-01-19
基金项目: 国家自然科学基金(No. 60474038)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

序列的均值为: $\bar{x} = E\{x\} = 0.5$, 所以可以通过门限函数 $n_0(x)$ 把实值混沌序列 $x_0, x_1, \cdots, x_n$ 转化为二进制"0"和"1"序列 $b_0, b_1, \cdots, b_n$.

$$n_0(x) = \begin{cases} 1, & x \geqslant 0.5 \\ 0, & x < 0.5 \end{cases}$$

### 2.2 块不相关水印技术

为了提高对水印图像篡改的检测和定位的精度, 往往采用块不相关水印技术, 该类算法的优点在于算法简单, 定位精度高.

块不相关水印技术可以简单描述为: 在隐藏水印信息 $\boldsymbol{W}$ 之前, 将原始作品 $\boldsymbol{C}_o$ 分为不相关的子块 $\{\boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_n\}$, 然后将水印信息 $\boldsymbol{W}_i$ 依据密钥 $k$ 独立地嵌入到子块 $\boldsymbol{C}_i$ 中, 结果记为 $\boldsymbol{C}_i'$, 其中 $\boldsymbol{C}_i'$ 完全取决于 $\boldsymbol{C}_i$、$\boldsymbol{W}_i$ 和密钥 $k$.

块不相关水印技术存在安全缺陷, 由于密钥和水印信息资源数量的有限性, 对于密钥和所嵌入的信息完全相同的情况下, 同一位置可能会隐藏相同的水印信息, 所以攻击者交换两个可信图像的同一位置的图像块后, 不会影响提取的水印信息. 为了提高算法的安全性, 文献[2]提出可以采用一些措施, 诸如生成与图像内容有关的水印信息或构造与图像特征有关的合成密钥.

## 3 基于 Logistic 映射的 DCT 水印嵌入算法

### 3.1 水印的产生

考虑一幅 $N \times N$ 的原始图像 $\boldsymbol{C}$, 水印的产生步骤如下:

(1) 将其划分为 $(M)^2$ 个 $8 \times 8$ 的小块, $M = N/8$, 分别记作 $\boldsymbol{C}_o^{(m,n)}$, $m = 1, 2, \cdots, M$; $n = 1, 2, \cdots, M$. 即

$$\boldsymbol{C}_o = \begin{pmatrix} \boldsymbol{C}_o^{(1,1)} & \boldsymbol{C}_o^{(1,2)} & \cdots & \boldsymbol{C}_o^{(1,M)} \\ \boldsymbol{C}_o^{(2,1)} & \boldsymbol{C}_o^{(2,2)} & \cdots & \boldsymbol{C}_o^{(2,M)} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{C}_o^{(M,1)} & \boldsymbol{C}_o^{(M,2)} & \cdots & \boldsymbol{C}_o^{(M,M)} \end{pmatrix} \tag{3}$$

将这种分块方式记作 $\boldsymbol{C}_o = (\boldsymbol{C}_o^{(m,n)})_{M \times M}$.

(2) 对每一个小块 $\boldsymbol{C}_o^{(m,n)}$ 进行二维 DCT 变换, 结果记为 $\boldsymbol{V}_o^{(m,n)}$.

$$\boldsymbol{V}_o^{(m,n)} = \begin{pmatrix} \boldsymbol{V}_{oLL}^{(m,n)} & \boldsymbol{V}_{oLH}^{(m,n)} \\ \boldsymbol{V}_{oHL}^{(m,n)} & \boldsymbol{V}_{oHH}^{(m,n)} \end{pmatrix} \tag{4}$$

其中 $\boldsymbol{V}_{oLL}^{(m,n)}$, $\boldsymbol{V}_{oLH}^{(m,n)}$, $\boldsymbol{V}_{oHL}^{(m,n)}$, $\boldsymbol{V}_{oHH}^{(m,n)}$ 均为 $4 \times 4$ 的矩阵, 分别为 $\boldsymbol{V}_o^{(m,n)}$ 的低频、中频、次高频和高频系数. 由这些系数合成的低频、中频、次高频和高频系数分别记为: $\boldsymbol{V}_{oLL} = (\boldsymbol{V}_{oLL}^{(m,n)})_{M \times M}$, $\boldsymbol{V}_{oLH} = (\boldsymbol{V}_{oLH}^{(m,n)})_{M \times M}$, $\boldsymbol{V}_{oHL} = (\boldsymbol{V}_{oHL}^{(m,n)})_{M \times M}$ 和 $\boldsymbol{V}_{oHH} = (\boldsymbol{V}_{oHH}^{(m,n)})_{M \times M}$

(3) 计算 $\boldsymbol{V}_{oHL}^{(m,n)}$ 各元素的算术平均值, 记为 $a^{(m,n)}$, 再计算 $\boldsymbol{V}_{oHL}^{(m,n)}$ 各元素的绝对值的最大值, 记为 $b^{(m,n)}$. 令

$$x_0^{(m,n)} = (|a^{(m,n)}|/b^{(m,n)} + k)/2$$

其中, $0 \leqslant |a^{(m,n)}|/b^{(m,n)} \leqslant 1$, $k$ 为水印密钥, $k \in (0, 1)$, 显然 $x_0^{(m,n)} \in (0, 1)$.

(4) 将得到的 $x_0^{(m,n)}$ 和 $\lambda = 4$ 作为 logistic 混沌映射的初始值和参数, 代入 logistic 映射迭代式(1), 生成一个长度为 16 的实值混沌序列 $x_0^{(m,n)}, x_1^{(m,n)}, \cdots, x_{15}^{(m,n)}$, 通过门限函数 $n_0(x)$ 把实值混沌序列 $x_0^{(m,n)}, x_1^{(m,n)}, \cdots, x_{15}^{(m,n)}$ 转化为二进制序列 $b_0^{(m,n)}, b_1^{(m,n)}, \cdots, b_{15}^{(m,n)}$.

从而得到一个 $4 \times 4$ 的水印信息, 记作 $\boldsymbol{W}_o^{(m,n)}$, 即:

$$\boldsymbol{W}_o^{(m,n)} = \begin{pmatrix} b_0^{(m,n)} & b_1^{(m,n)} & b_2^{(m,n)} & b_3^{(m,n)} \\ b_4^{(m,n)} & b_5^{(m,n)} & b_6^{(m,n)} & b_7^{(m,n)} \\ b_8^{(m,n)} & b_9^{(m,n)} & b_{10}^{(m,n)} & b_{11}^{(m,n)} \\ b_{12}^{(m,n)} & b_{13}^{(m,n)} & b_{14}^{(m,n)} & b_{15}^{(m,n)} \end{pmatrix} \tag{5}$$

那么图像的水印信息 $\boldsymbol{W}_o = (\boldsymbol{W}_o^{(m,n)})_{M \times M}$.

由于混沌初值是由水印密钥和次高频系数合成的, 每个水印信息 $\boldsymbol{W}_o^{(m,n)}$ 都和相应块的次高频系数有关, 并利用了混沌映射对初值的敏感性, 使得不同图像的相同子块或同一图像的不同子块下的水印信息都不可能相同, 这样可以防止通过交换两个可信图像的相同子块或同一图像的不同子块而不影响水印信息的提取这种攻击, 有效地克服了块不相关技术存在的这种安全性缺陷.

### 3.2 水印的嵌入

图像的 DCT 高频系数 $\boldsymbol{V}_{oHH}$ 是图像感知中最不重要的分量, 但它对图像的修改却最为敏感, 所以将生成的水印信息 $\boldsymbol{W}_o$ 按下列方法嵌入到图像的 DCT 高频系数 $\boldsymbol{V}_{oHH}$ 中:

$$\boldsymbol{V}_{oHH}' = \boldsymbol{V}_{oHH} + \boldsymbol{D}$$

其中, $\boldsymbol{D}(i,j) = \boldsymbol{a}(i,j) \times \boldsymbol{W}_o(i,j)$, $i = 1, 2, \cdots, N/2$; $j = 1, 2, \cdots, N/2$, $\alpha$ 是嵌入强度. 为了实现水印的盲检测我们取嵌入强度 $\alpha = \tau + \boldsymbol{V}_{oHL} - \boldsymbol{V}_{oHH}$, 其中, $\tau$ 的每一个元素均等于水印的检测值 $\tau$. 所以:

(1) 如果 $\boldsymbol{W}_o(i,j) = 1$, 则

$$\begin{aligned} \boldsymbol{V}_{oHH}'(i,j) &= \boldsymbol{V}_{oHH}(i,j) + \alpha(i,j)\,\boldsymbol{W}_o(i,j) \\ &= \boldsymbol{V}_{oHH}(i,j) + \alpha(i,j) \\ &= \boldsymbol{V}_{oHH}(i,j) + \tau + \boldsymbol{V}_{oHL}(i,j) - \boldsymbol{V}_{oHH}(i,j) \\ \Rightarrow \boldsymbol{V}_{oHH}'(i,j) - \boldsymbol{V}_{oHL}(i,j) &= \tau \end{aligned}$$

(2) 如果 $\boldsymbol{W}_o(i,j) = 0$, 则

$$\boldsymbol{V}_{oHH}'(i,j) = \boldsymbol{V}_{oHH}(i,j) + \alpha(i,j)\,\boldsymbol{W}_o(i,j) = \boldsymbol{V}_{oHH}(i,j)$$

这样我们就可以得到改变后的图像 DCT 系数 $\boldsymbol{V}_o'$:

$$\boldsymbol{V}_o' = \begin{pmatrix} \boldsymbol{V}_{oLL} & \boldsymbol{V}_{oLH} \\ \boldsymbol{V}_{oHL} & \boldsymbol{V}_{oHH}' \end{pmatrix}$$

再将 $\boldsymbol{V}_o'$ 经过 IDCT 变换得到水印图像 $\boldsymbol{C}_w$.

一个 $8 \times 8$ 的小块 $\boldsymbol{C}_o^{(m,n)}$ 水印嵌入过程如图 1 所示, 图中的符号均属于一个 $8 \times 8$ 的小块, 为了简便, 省略了上标 $(m, n)$.

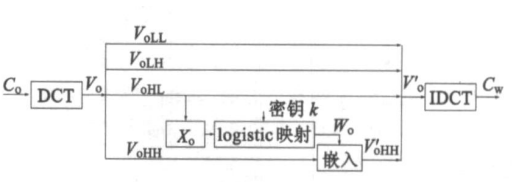



图 1　水印嵌入过程示意图

### 3.3 水印的检测

首先水印图像 $\boldsymbol{C}_w$ 经过水印的产生步骤(1)和(2), 得到

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

水印图像的高频系数 $V_{wHH}$ 和次高频系数 $V_{wHL}$, 然后根据水印密钥经过步骤(3)和(4)提取出水印信息 $W'_o$.

定义篡改判别矩阵:

$$A(i,j)=\begin{cases}1, & V_{wHH}(i,j)-V_{wHL}(i,j)=\tau\\ 0, & V_{wHH}(i,j)-V_{wHL}(i,j)\neq\tau\end{cases} \quad (6)$$

如果 $A(i,j)\neq W'_o(i,j)$, 那么原始水印信息 $W_o(i,j)$ 被篡改了, $i=1,2,\cdots,N/2$; $j=1,2,\cdots,N/2$. 映射为图像的第 $(m,n)$ 个 $8\times 8$ 的块中至少有一个像素点被篡改, 其中

$$m=\lfloor (i-1)/4\rfloor+1,\ n=\lfloor (j-1)/4\rfloor+1$$

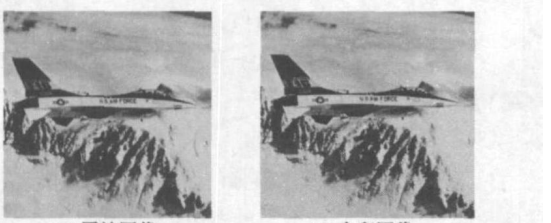
如果图像的任一像素点被篡改了, 它将引起混沌初值的改变, 由于混沌对初值非常敏感, 即使改变很小, 也将得到完全不同的水印信息, 根据篡改判别矩阵, 可检测并定位对水印图像的篡改区域.

## 4 实验结果

为了说明本文算法的有效性, 给出了该算法的几个 Matlab 仿真结果. 所有的仿真都是基于两个大小均为 512× 512 的原始图像"Lena"和"Airplane"进行的, 如图 2(a)和图 3(a)所示. 取水印密钥 $k=0.1$, $\lambda=4$, 和检测值 $\tau=0.1$, 得到的水印图像如图 2(b)和图 3(b)所示.

(a)原始图像 (b)水印图像

图 2 "Lena"图像



(a)原始图像 (b)水印图像

图 3 "Airplane"图像

### 4.1 水印的嵌入有效性

在水印系统没有受到任何攻击的情况下, 水印系统的有效性就是嵌入水印后能正确检测到水印的概率. $W_o(i,j)$ 为原始水印信息, $W'_o(i,j)$ 为提取的水印信息. 根据本文提出的嵌入和检测算法可知:

$$P(W'_o(i,j)=1\mid W_o(i,j)=1)=1$$

$$P(W'_o(i,j)=0\mid W_o(i,j)=0)=1-P_o$$

其中, $P_o$ 为 $V_{oHH}(i,j)-V_{oHL}(i,j)=\tau$ 的概率. 所以水印系统的有效性为 $1-P_o$. 然而, 实际测得"Lena"和"Airplane"的嵌入有效性均为 100%.

### 4.2 水印的不可见性

脆弱水印的第一个重要特性是不可见性. 为了衡量水印图像和原始图像的差别, 水印图像和原始图像之间的峰值信噪比 PSNR 定义为:

$$\mathrm{PSNR}=10\log_{10}\left\{\frac{255^2}{\frac{1}{N\times N}\sum_{i=1}^{N}\sum_{j=1}^{N}(C_w(i,j)-C_o(i,j))^2}\right\} \quad (7)$$

水印图像"Lena"和"Airplane"的 PSNR 分别为 45.2520 和 43.0918.

由于水印信息和密钥 $k$ 有关, 嵌入强度与检测值 $\tau$ 有关, 它们都将影响到 PSNR, 所以有必要测试 PSNR 随密钥 $k$ 和检测值 $\tau$ 的变化, 如图 4 和图 5 所示.

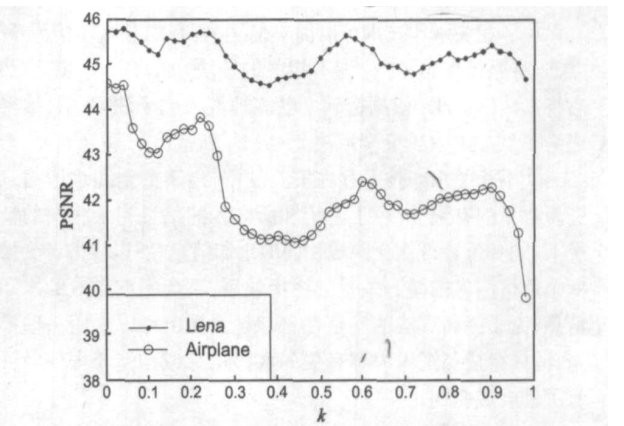



图 4 PSNR 随 $k$ 的变化

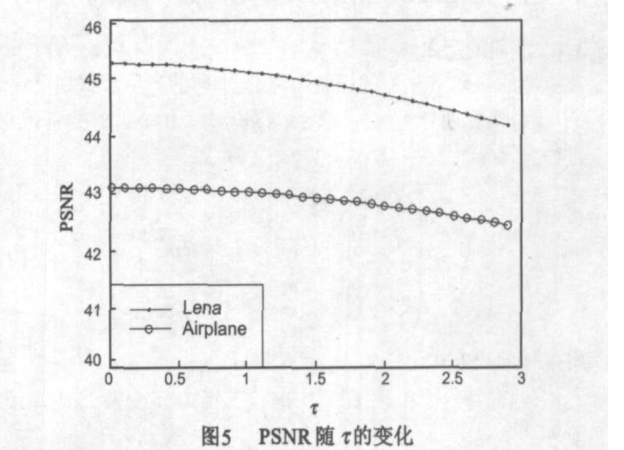
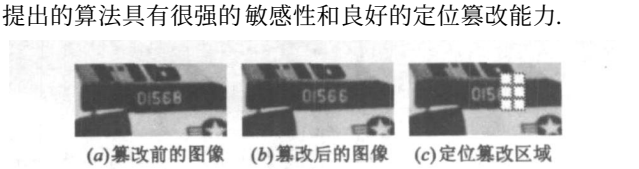



图5 PSNR 随 $\tau$ 的变化

由图可以看出, PSNR 值随密钥 $k$ 出现波动, 波动的幅度和原始图像有关. PSNR 随检测值 $\tau$ 的变化呈现总体的下降, 另外, PSNR 在 $\tau\in[0,1]$ 区间内的值最大且基本稳定, 所以最好取 $\tau\in[0,1]$.

### 4.3 篡改的敏感性和定位能力

为了测试算法对图像篡改的敏感性和定位篡改能力, 将"Airplane"图像中机翼上的数字"01568"篡改为"01566", 篡改定位检测的结果如图 6 所示, 图 6(a)、图 6(b)和图 6(c)是检测"Airplane"图像篡改区域前后的放大的结果. 实验表明本文提出的算法具有很强的敏感性和良好的定位篡改能力.



(a)篡改前的图像 (b)篡改后的图像 (c)定位篡改区域

图 6 "Airplane"图像的篡改区域检测

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

## 5 结论

提出了混沌应用在脆弱数字水印中的一个新的算法, 将图像 DCT 系数和密钥结合起来映射为 Logistic 映射的初值生成水印, 并利用图像 DCT 系数之间的关系, 实现了水印的嵌入和盲检测. 该算法计算简单, 具有较高的峰值信噪比和良好的篡改定位能力. 如果将该算法中的次高频系数改为低频系数, 就可能区分 JPEG 和低通滤波等一些常规处理和恶意攻击, 如何设计出此类的半脆弱数字水印算法是本文以后研究的一个重要方向.

参考文献:

[1] 丁科, 何晨, 王宏霞. 一种定位精确的混沌脆弱数字水印技术[J]. 电子学报, 2004, 32(6): 1009- 1012.
Ding Ke, He Chen, Wang Hong-xia. A chaotic fragile watermarking technique with precise localization[J]. Acta Electronica Sinica, 2004, 32(6): 1009- 1012. (in Chinese)

[2] 张小华, 孟红云, 刘芳, 焦李成. 一类有效的脆弱型数字水印技术[J]. 电子学报, 2004, 32(1). 114- 117.
Zhang Xiao-hua, Meng Hong-yun, Liu Fang, Jiao Li-cheng. A new kind of efficient fragile watermarking technique[J]. Acta Electronica Sinica, 2004, 32(1): 114- 117. (in Chinese)

[3] Jui-Cheng Yen. Watermark embedded in the permuted image [A]. Proc of 2001 IEEE International Conference on Circuits and Systems: Symposium[C]. Sydney, NSW: IEEE, 2001, 2: 53 - 56.

[4] Tefas A, Pitas L. Image authentication using chaotic mixing systems[A]. Proc of 2000 IEEE International Conference on Circuits and Systems: Symposium[C]. Geneva: IEEE, 2000, 1: 216 - 219.

[5] Voyatzis G, Pitas I. Chaotic watermarks for embedding in the spatial digital image domain[A]. Proc of 1998 IEEE International Conference on Image Processing[C]. Chicago, IL: IEEE, 1998, 2: 432- 436.

[6] Chi Kin Ho. Chang-Tsun Li. Semi-fragile watermarking scheme for authentication of JPEG images[A]. Proc of 2004 IEEE International Conference on Information Technology: Coding and Computing[C]. IEEE, 2004, 1: 7- 11

作者简介:

李赵红　女, 1982 年 11 月出生于江西丰城, 博士研究生, 主要研究方向为非线性理论及数字水印技术. E-mail: zhaohong. li@ 126. com

侯建军　男, 1957 年 8 月出生于天津市, 博士生导师, 主要研究方向为非线性理论及其应用研究.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net