Journal of Image and Signal Processing 图像与信号处理, 2019, 8(2), 83-89
Published Online April 2019 in Hans. http://www.hanspub.org/journal/jisp
https://doi.org/10.12677/jisp.2019.82012

Hans汉斯

Multi-Image Watermarking Algorithm Based on Secret Sharing and Histogram Shifting

Zhuoying Zhao[1,2], Jiazhi Zhang[1,2], Xiaoqiang Zhang[1,2*]

[1]School of Information and Control Engineering, China University of Mining and Technology, Xuzhou Jiangsu
[2]Xuzhou Key Laboratory of Artificial Intelligence and Big Data, Xuzhou Jiangsu
Email: *grayqiang@163.com

Received: Apr. 3rd, 2019; accepted: Apr. 14th, 2019; published: Apr. 28th, 2019

Abstract

To solve the problems of small embedding capacity and low security of image watermarking algorithm, a watermarking image can be decomposed into multiple shadow images with the secret sharing algorithm, and then the shadow images can be embedded into multiple carrier images by histogram shifting. This paper proposes a multi-image watermarking algorithm based on secret sharing and histogram shifting. In this algorithm, the watermarking image cannot be extracted by only one shadow image, and other shadow images must be used. Therefore, the algorithm security is improved. Meanwhile, the embedding capacity of image watermarking can be enlarged by increasing the number of carrier images. Algorithm analyses and experimental results show that the proposed algorithm is feasible.

Keywords

Image Watermarking, Secret Sharing, Histogram Shifting, Multiple Image Process

基于秘密分享和直方图平移的多图像水印算法

赵卓影[1,2]，张佳志[1,2]，张晓强[1,2*]

[1]中国矿业大学信息与控制工程学院，江苏 徐州
[2]徐州市人工智能与大数据重点实验室，江苏 徐州
Email: *grayqiang@163.com

收稿日期：2019年4月3日；录用日期：2019年4月14日；发布日期：2019年4月28日

摘 要

针对目前图像水印算法存在的嵌入容量小和安全性弱的问题，利用秘密分享方案将一幅水印图像分解成

*通讯作者。

文章引用: 赵卓影, 张佳志, 张晓强. 基于秘密分享和直方图平移的多图像水印算法[J]. 图像与信号处理, 2019, 8(2): 83-89. DOI: 10.12677/jisp.2019.82012

多幅影子图像，再通过直方图平移算法把影子图像分别嵌入到多幅载体图像中，从而提出了一种基于秘密分享和直方图平移的多图像水印算法。在该算法中，若仅有一幅影子图像将无法提取出水印图像，需要有其他影子图像，从而提高了图像水印算法的安全性。同时，通过增加载体图像的数量，可扩大图像水印算法的嵌入容量。算法分析和实验结果表明该算法的可行性。

关键词

图像水印，秘密分享，直方图平移，多图像处理

1. 引言

图像是网络信息的重要载体。据心理学家统计，人类约有 70%的信息都来自视觉。拍摄设备的增加以及拍摄的便捷性使得图像在军事、医疗、气象、电子政务以及个人事务等领域得到了广泛的应用。人们的图像版权保护意识逐渐增强，图像水印是一种保护图像版权的技术。然而，黑客攻击能力的提升以及图像复制和传播的便捷，对图像水印技术提出了新挑战。

秘密分享方案[1] [2]是利用 Shamir 的(k,n)门限秘密分享机制。它是将一份秘密信息分解成n份影子信息，任何一份影子信息均无法独自恢复出秘密信息，只有把其中的任意$k\left(k\le n\right)$份影子信息联合起来才能恢复出秘密信息。

对于基于直方图平移的可逆水印算法，高峰值点意味着较高的嵌入能力[3]。在直方图可逆水印技术中，利用峰值点和零值点对来修改载体图像的直方图。可嵌入到载体图像中的秘密位数等于与峰值点相关联的像素数。在覆盖图像块上应用模量算子后，利用载体图像的直方图来确定嵌入位置。使用模量算子的主要目的是增加载体图像直方图中的峰值点数，这增加了载体图像的嵌入能力，而含水印图像的失真度较低[4]。单幅图像水印算法仅有一幅载体图像，水印嵌入容量有限。多图像水印算法含有多幅载体图像，可明显扩大嵌入容量。目前，多图像水印技术越来越受到研究者们的关注[5]。

因此，将秘密分享方案和基于直方图平移的图像水印算法有机地结合，提出一种基于秘密分享和直方图平移的多图像水印算法。算法分析和实验结果表明：该算法是安全可靠的，且具有较大的嵌入容量。

2. 理论基础

2.1. 秘密分享方案

Shamir 的(k,n)门限秘密分享方案的基本思想是：首先，要把秘密S分割成n份影子信息；其次，分别将n份影子信息分发给n个参与者进行保管；最后，任意$k\left(k\le n\right)$份影子信息联合起来才能恢复出S。

基于拉格朗日插值多项式算法的秘密分享方案[6]描述如下。令$k-1$次的拉格朗日多项式为：

$$f\left(x\right)=m_0+m_1x+m_2x^2+\cdots+m_{k-1}x^{k-1},\tag{1}$$

其中，k为整数且$k\le n$，系数$m_1,m_2,\cdots,m_{k-1}$可根据情况任意选取[7]。

令水印图像为秘密 S，则基于拉格朗日插值多项式算法的秘密分享方案可描述为：将一幅水印图像

分解成 n 幅影子图像，任何一幅影子图像均无法独自恢复出水印图像，只有把其中的任意 $k\left(k\le n\right)$ 份影子联合起来才能恢复出水印图像。

2.2. 直方图平移算法

Ni 等人提出了一种基于直方图平移的可逆水印算法[8]，其算法思想为：首先，绘出图像的灰度直方图，并找出其中的最大值点 a 和最小值点 b，为方便讨论，不妨设 $a<b$；其次，将图像中所有在 $\left[a+1,b-1\right]$ 的灰度值加 1，即将 $\left[a+1,b-1\right]$ 的直方图向右平移一位，从而像素值为 $a+1$ 的像素点的个数变为 0；再次，在嵌入水印时，若水印值为 1，则像素值为 a 的灰度值加 1，即为 $a+1$；若水印值为 0，则保持 a 的像素值不变；最后，提取水印信息时，顺序扫描图像，若像素灰度值为 a，则提取的水印信息为 0；若像素灰度值为 $a+1$，则提取的水印信息为 1 [9]。若想恢复出原始宿主图像，只需把灰度值处在区间 $\left[a+1,b\right]$ 的灰度值减 1 即可。

3. 新多图像水印算法

3.1. 生成影子图像

设水印图像为 W，根据基于拉格朗日插值多项式算法的秘密分享方案，生成 n 幅影子图像步骤如下：

步骤 1：令公式(1)中的 $m_0=w_{ij}$，其中 $w_{ij}\in W$；

步骤 2：随机选取 $m_1,m_2,\cdots,m_{k-1}$ 的值作为公式(1)的系数；

步骤 3：选择 W 上 n 个不同的非零值 $x_1,x_2,\cdots,x_n$，且将此 n 个值公开，分别计算 $w_{ij}^1=f\left(x_1\right),w_{ij}^2=f\left(x_2\right),\cdots,w_{ij}^n=f\left(x_n\right)$；

步骤 4：对 W 中的所有像素进行步骤 1~步骤 3 的操作，即可得到 n 幅影子图像，即 $W^1=\left\{w_{ij}^1\right\},W^2=\left\{w_{ij}^2\right\},\cdots,W^n=\left\{w_{ij}^n\right\}$。

3.2. 嵌入影子图像

设 $k\left(k\le n\right)$ 幅载体图像为 $I_1,I_2,\cdots,I_k$，从 n 幅影子图像中任选 k 幅即 $W^1,W^2,\cdots,W^k$ 作为水印信息，分别嵌入到 k 幅载体图像中。根据秘密分享方案，k 幅影子图像可以恢复出原水印图像。提出的多图像水印算法嵌入影子图像的详细步骤如下：

步骤 1：绘制 I_1 的直方图，找出其中的最大值点 a，并在最大值点右侧寻找最小值点 b [10]；

步骤 2：直方图平移。在像素值为 $\left[a,b\right]$ 内的像素点上嵌入影子信息，先顺序扫描图像，当扫描到的像素值为 $\left[a+1,b-1\right]$ 内的值时，将其值加上 1，其他的像素值不变；

步骤 3：嵌入影子。扫描载体图像，当扫描到的像素值为 a 时，在该像素点嵌入 1 位影子信息 $w_{ij}^1\in W^1$ 且 $w_{ij}^1\in\left\{0,1\right\}$。嵌入规则为：若嵌入的水印影子信息为 0，则该点像素值不变；若嵌入的影子信息为 1，则该点的像素值加 1；

步骤 4：类似地，将影子图像 $W^2,W^3,\cdots,W^k$ 分别嵌入到 $I_2,I_3,\cdots,I_k$，最终可得含水印图像为 $I_1^W,I_2^W,\cdots,I_k^W$。

3.3. 提取影子图像及恢复载体图像

步骤 1：提取影子图像。对含水印图像 I_1^W 的像素值进行顺序扫描，若扫描到的像素值为 a，则恢复的影子信息为“0”；若扫描到的像素值为 $a+1$，则恢复的影子信息为“1”，从而恢复出影子图像 W^1。类似地，可提取出含水印图像 $I_2^W,I_3^W,\cdots,I_k^W$ 中的 $k-1$ 幅影子图像 $W^2,W^3,\cdots,W^k$；

步骤 2：将 k 组不同的值 $\left(x_1, w_{ij}^1\right), \left(x_2, w_{ij}^2\right), \cdots, \left(x_k, w_{ij}^k\right)$ 分别代入公式(1)可得如下方程组，其中，$w_{ij}^1 \in W^1, w_{ij}^2 \in W^2, \cdots, w_{ij}^k \in W^k$，为影子图像 (i, j) 位置的像素值，

$$\begin{cases} w_{ij}^1\left(x_1\right) = m_0 + m_1 x_1 + m_2 x_1^2 + \cdots + m_{k-1} x_1^{k-1} \bmod 255 \\ w_{ij}^2\left(x_2\right) = m_0 + m_1 x_2 + m_2 x_2^2 + \cdots + m_{k-1} x_2^{k-1} \bmod 255 \\ \vdots \\ w_{ij}^p\left(x_k\right) = m_0 + m_1 x_k + m_2 x_k^2 + \cdots + m_{k-1} x_k^{k-1} \bmod 255 \end{cases}; \quad (2)$$

步骤 3：通过求解方程组式(2)的解就能得到所需要的 $m_0, m_1, m_2, \cdots, m_{k-1}$ 的值，其中 m_0 就是要恢复水印图像的像素值，将其存储在需要恢复水印图像的相应位置。类似地，对每个像素进行处理，最后能恢复出水印图像[11] [12]；

步骤 4：恢复载体图像。再次顺序扫描图像，将扫描到的 $[a+1, b]$ 内的像素值减去 1，即可恢复载体图像。

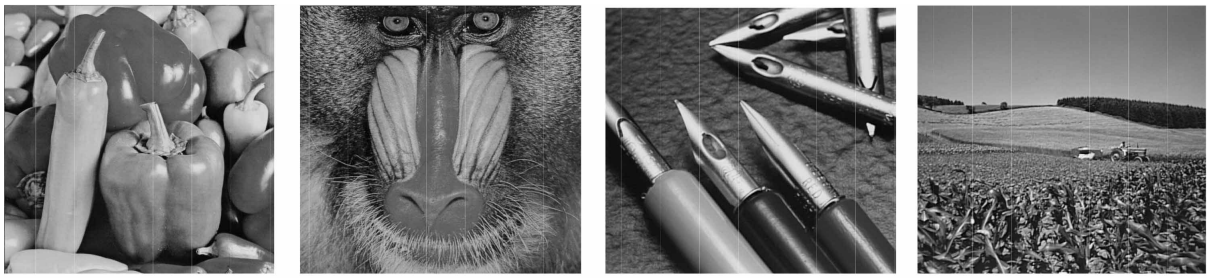
4. 实验验证

选取大小为 50×50 的 Lena 灰度图像作为水印图像，根据 3.1 节影子图像生成算法可生成 8 幅影子图像，如图 1 所示。选取大小均为 512×512 的 Pepper，Baboon 和 Pens 等 8 幅载体图像，如图 2 所示。根据 3.2 节嵌入影子图像算法，将 8 幅影子图像分别嵌入到 8 幅载体图像中，得到含水印图像，如图 3 所示。提取出 8 幅影子图像后，根据 3.3 节提取影子图像及恢复载体图像算法，提取的水印图像，如图 4 所示。

(a) 影子图像 1　(b) 影子图像 2　(c) 影子图像 3　(d) 影子图像 4

(e) 影子图像 5　(f) 影子图像 6　(g) 影子图像 7　(h) 影子图像 8

Figure 1. Shadow images
图 1. 影子图像



(a) Pepper　(b) Baboon　(c) Pens　(d) Cornfield

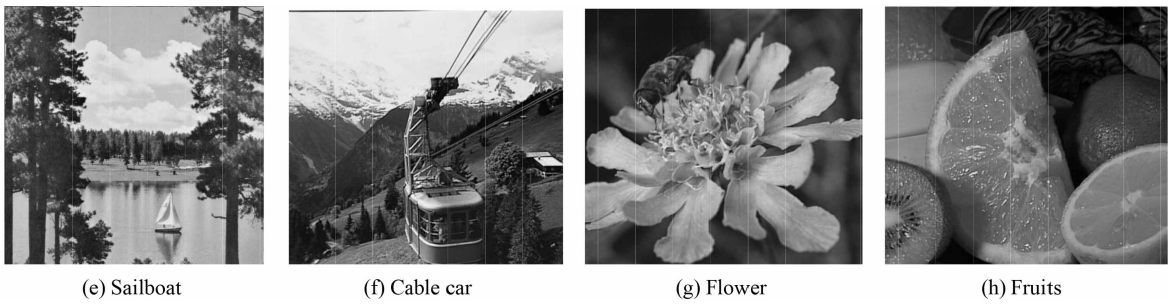


Figure 2. Carrier images
图 2. 载体图像

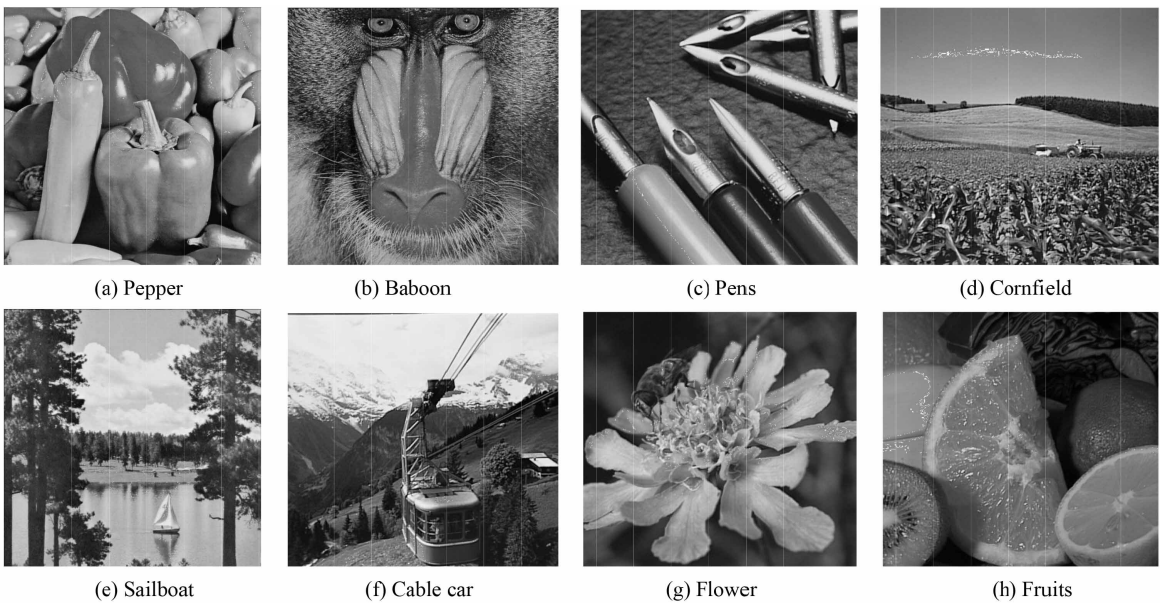


Figure 3. Watermarked images
图 3. 含水印图像

Figure 4. Extracted watermark image
图 4. 提取的水印图像

5. 算法分析

透明性、鲁棒性、安全性、嵌入容量和算法执行效率是评价图像水印算法主要性能指标[13]。

5.1. 透明性

透明性是指数字水印的嵌入不能影响图像的正常使用，不会引起人类视觉系统的察觉。透明性可通过

人眼进行主观评价或利用峰值信噪比(Peak Signal-to-Noise Ratio，简称 PSNR)进行客观评价。PSNR 定义为：

$$\mathrm{PSNR}=10\lg\frac{255^2}{\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(X(i,j)-X_W(i,j)\right)^2} \tag{3}$$

其中，$X(i,j)$为原始图像的像素值，$X_W(i,j)$为含水印图像的像素值。PSNR 值越小，则表示图像质量下降越多，透明性越差。反之，其值越大，透明性越好。

实验测得，图 3 所示的含水印图像对应的 PSNR 平均值 30.86。虽然该数值偏小些，但是基于直方图平移的图像水印算法是一种可逆水印技术，可无损地恢复出原始载体图像。

5.2. 鲁棒性

鲁棒性是指含水印图像在经过常规信号处理操作后仍能检测水印的能力。针对图像的常规操作包括空间滤波、JPEG 压缩、剪切攻击、打印与复印、几何变形和噪声攻击等。鲁棒性评价一般由归一化相关系数(Normalized Correlation，简称 NC)来衡量。NC 的定义为：

$$\mathrm{NC}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}W(i,j)W'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}W^2(i,j)} \tag{4}$$

其中，W 表示原始水印图像，W'为提取的水印图像。NC 越接近于 1，则表明提取的水印就越接近于原始水印，水印算法的鲁棒性越健壮。

在无噪声的情况下，计算图 4 和图 1 对应的 NC 的值为 1，即提取的水印图像与原始水印图像完全相同。同时，通过对图像的 JPEG 压缩、裁剪攻击和高斯噪声攻击等测试，表明了新算法具有良好的鲁棒性。

5.3. 安全性

安全性是指水印算法能够抵抗各种破坏水印行为的能力，即未授权者不能去除、嵌入和检测水印。同时，水印信息应该很难被他人复制和伪造。

新算法利用了秘密分享的方案，将一幅水印图像分解成 n 幅影子图像。在提取水印时，必须由 p 份影子图像联合起来才能提取出水印图像，从而提高了图像水印算法的安全性。

5.4. 嵌入容量

嵌入容量是指采用水印算法能嵌入水印信息的多少。人们期望水印算法具有较大的嵌入容量。新算法将 p 幅影子图像分别嵌入到 p 幅载体图像中，从而扩大了水印算法的嵌入容量。同时，用户也可根据实际应用需要，通过调整载体图像的幅数，来控制嵌入容量的大小。

5.5. 算法执行效率

算法的时间复杂度是衡量算法执行效率的重要依据，通常用函数$T(n)$来表示。

在生成影子图像时，须构造一个 $k-1$ 次拉格朗日多项式，如公式(1)所示。其时间复杂度 $T(n)=O\left(n^{k-1}\right)$。在提取水印图像时，须构造拉格朗日方程组，如公式(2)所示。其时间复杂度为 $T(n)=O\left(n^{k-1}\right)$。

同时，在影子图像嵌入过程中，主要包括像素比较、像素扫描和像素平移三个操作，其复杂度分析为：1) 需要$(n-1)$次像素比较来确定峰值点和零值点，其中 n 为灰度级数；2) 令图像大小 size，则需要

进行 size 次像素扫描；3) $\sum_{i\in(\text{peak\_point},\text{zero\_point})} h(i)$ 次像素平移和一半数量峰值点向零点变化的加法操作 $\frac{1}{2}h(\text{peak\_point})$。其中，$h(i)$ 为直方图函数，peak_point 为峰值点，zero_point 为零点。因此，嵌入水印算法的复杂度为：

$$T(n)=O\left((n-1)+\text{size}+\sum_{i\in U(\text{peak\_point},\text{zero\_point})} h(i)+\frac{1}{2}h(\text{peak\_point})\right) \tag{5}$$

对于实际图像，由于 size 远大于 n，故嵌入操作的时间复杂度近似为 $T(n)=O(\text{size})$ [14]。

实验测得，将 1 幅影子图像嵌入到 1 幅载体图像中平均耗时为 0.36 秒。说明新算法是高效的。

6. 结论

将秘密分享方案与基于直方图平移的图像水印算法有机结合，提出一种基于秘密分享和直方图平移的多图像水印算法。该算法利用秘密分享方案提高了水印算法的安全性。同时，通过增加载体图像幅数，增大了水印算法的嵌入容量。算法分析和实验结果表明，提出的多图像水印算法具有良好的鲁棒性、安全性和高效性。

致　谢

非常感谢国家自然科学基金“大容量高安全的加密域图像可逆水印算法研究”(61501465)和江苏省大学生创新训练项目“加密域图像可逆水印算法研究”(201810290059X)对该文的资助。感谢匿名审稿人对论文提出建设性的修改意见。

参考文献

[1] 张景中, 陈亮, 滕鹏国, 王晓京. 一种基于阵列码的图像秘密分享方法[J]. 四川大学学报(工程科学版), 2016, 48(6): 140-148.

[2] Ding, H.Y., Li, Z.C. and Bi, W. (2018) (k,n) Halftone Visual Cryptography Based on Shamir's Secret Sharing. *The Journal of China Universities of Posts and Telecommunications*, **25**, 60-76.

[3] 吴万琴, 阮文惠, 贺元香. 一种基于直方图平移和局部复杂度的可逆水印算法[J]. 南京师大学报(自然科学版), 2016, 39(3): 33-39.

[4] 于爽, 李健. 基于直方图平移的鲁棒可逆信息隐藏方案[J]. 武汉大学学报(工学版), 2018, 51(3): 268-275+282.

[5] 孙鹤鹏, 张晓强. 基于 DNA 编码的多图像加密算法[J]. 计算机工程与设计, 2018, 39(10): 3050-3054+3099.

[6] Bao, L., Yi, S. and Zhou, Y.C. (2017) Combination of Sharing Matrix and Image Encryption for Lossless (k,n)-Secret Image Sharing. *IEEE Transactions on Image Processing*, **26**, 5618-5631. https://doi.org/10.1109/tip.2017.2738561

[7] Ding, H.Y., Li, Z.C. and Bi, W. (2018) (k,n) Halftone Visual Cryptography Based on Shamir's Secret Sharing. *The Journal of China Universities of Posts and Telecommunications*, **25**, 60-76.

[8] Ni, Z.C., Shi, Y.Q., Ansari, N. and Su, W. (2006) Reversible Data Hiding. *IEEE Transactions on Circuits and Systems for Video Technology*, **16**, 354-362. https://doi.org/10.1109/TCSVT.2006.869964

[9] 李雪景, 李江隐, 康宝生. 基于图像插值和直方图平移的可逆水印算法[J]. 计算机应用研究, 2016, 33(4): 1159-1163.

[10] 罗昊, 谢晓尧, 彭长根. 基于直方图平移的加密域可逆水印算法[J]. 郑州大学学报(理学版), 2018, 50(2): 29-34.

[11] 谭亦夫, 李子臣. 基于 Shamir 门限秘密分享的图像可视加密算法[J]. 网络与信息安全学报, 2018, 4(7): 69-76.

[12] Li, M., Yu, J. and Hao, R. (2017) A Cellular Automata Based Verifiable Multi-Secret Sharing Scheme without a Trusted Dealer. *Chinese Journal of Electronics*, **26**, 313-318. https://doi.org/10.1049/cje.2017.01.026

[13] 张晓强, 王蒙蒙, 朱贵良. 图像水印算法研究新进展[J]. 计算机工程与科学, 2012, 34(4): 17-22.

[14] 王俊祥, 杨波. 基于直方图平移可逆水印的性能估计[J]. 计算机应用, 2010, 30(12): 3246-3251.

知网检索的两种方式：

1. 打开知网页面 http://kns.cnki.net/kns/brief/result.aspx?dbPrefix=WWJD
   下拉列表框选择：[ISSN]，输入期刊 ISSN：2325-6753，即可查询
2. 打开知网首页 http://cnki.net/
   左侧“国际文献总库”进入，输入文章标题，即可查询

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：jisp@hanspub.org