

基于 SVD 和 ICA 的鲁棒水印算法^{*}

李海峰, 王树勋, 温 泉, 宋巍巍

(吉林大学通信工程学院, 吉林 长春 130025)

摘 要: 提出了一种新的基于 SVD (singular value decomposition, 奇异值分解) 和 ICA (independent component analysis, 独立分量分析) 的鲁棒水印算法。采用二值图像作为水印, 并进行 Arnold 变换, 提高了安全性。SVD 用于水印的嵌入过程, ICA 用于水印信号的提取。该算法的水印容量大大提高, 同时还保证了鲁棒水印的不可感知性。借助于 ICA, 该算法在不需考虑水印图像所经历的攻击类型及攻击参数的情况下, 能够正确提取水印信号。实验结果表明, 该算法对于 JPEG 压缩、噪声等具有鲁棒性, 尤其对于几何攻击如旋转、剪切、伸缩具有很好的鲁棒性。

关键词: 数字水印; 奇异值分解 (SVD); 独立分量分析 (ICA); Arnold 变换; 混沌序列;

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0053-05

数字水印是一种有效地数字产品版权保护和数据安全维护技术, 是信息隐藏技术领域的一个重要分支。数字水印技术利用数字作品中普遍存在的信息冗余性与随机性, 向其中嵌入可鉴别性的数字信号或模式, 而且并不影响宿主数据的可用性。任何数字水印都有三个基本要素: 水印本身的结构、嵌入水印的策略和水印的检测^[1]。

不同的应用对数字水印的要求是不尽相同的。不可感知性和鲁棒性是用于版权保护的两个最重要特性。同时, 水印嵌入量的大小也是衡量水印系统的一个重要指标。令人遗憾的是, 水印系统的这三个基本要求是相互制约的。

现有的大多数鲁棒水印算法着重于提高水印对各种攻击 (JPEG 压缩、剪切等) 的抵抗力, 通常以牺牲水印嵌入量为代价。为了在保证不可感知性的同时提高水印嵌入量, Bami^[2] 等人提出在水印系统中应用 HVS (human visual system 人类视觉系统), 但改进的效果不甚理想。本文提出的基于 SVD 和 ICA 的鲁棒水印算法, 在兼顾水印的不可感知性和鲁棒性的同时, 提高了水印的嵌入容量, 在水印系统的基本要求中取得了一个很好的折衷。

另外, 水印系统的安全性也是一个不容忽视的问题。本文算法首先用 Arnold 变换对水印信号 (二值图像) 进行置乱。密钥图像由混沌序列产生, 由于混沌序列具有初值敏感性, 从而保证了密钥的唯一性。

本文在第 2 节介绍了 SVD 和 ICA 的理论基础;

第 3 节给出了基于 SVD 和 ICA 的水印嵌入和提取算法; 第 4 节给出了本文算法与 Dan Yu 算法^[3] 的对比实验结果及讨论; 最后对全文进行了总结。

1 奇异值分解和独立分量分析

1.1 奇异值分解 (SVD)

奇异值分解是一种线性代数的工具, 在图像压缩、信噪分离等方面有着广泛的应用。大小为 $m \times n$ 的矩阵 $A \in C^{m \times n}$ 的奇异值分解为

$$A = U \Lambda V^H = \sum_{i=1}^r \lambda_i u_i v_i^H \quad (1)$$

其中, $U = (u_1, u_2, \dots, v_m) \in C^{m \times m}$, $V = (v_1, v_2, \dots, v_n) \in C^{n \times n}$ 是 2 个酉矩阵, $U^H U = E$, $V^H V = E$ 。... 表示一元素为非负数的对角阵, $r \leq \min\{m, n\}$ 是矩阵 A 的秩, $\lambda_1, \lambda_2, \dots, \lambda_r$ 称为矩阵 A 的奇异值 (SV)。 $\lambda_i = \sqrt{\mu_i}$, $i = 1, 2, \dots, r$, 其中 μ_i 是矩阵 $A^H A$ 或 $A A^H$ 的特征值。 u_i , $i = 1, 2, \dots, r$ 称为矩阵 A 的左奇异向量, 对应于矩阵 $A A^H$ 的特征向量。 v_i , $i = 1, 2, \dots, r$ 称为矩阵 A 的右奇异向量, 对应于矩阵 $A^H A$ 的特征向量。

1.2 独立分量分析 (ICA)

线性 ICA 混合模型描述为

$$X = AS \quad (2)$$

其中, $S = [s_1, s_2, \dots, s_n]^T$ 是相互独立的源信号矢量, $A = (a_{i,j})$, $i = 1, 2, \dots, m; j = 1, 2, \dots, n$ 是未知的混合矩阵, $X = [x_1, x_2, \dots, x_m]^T$ 是观测信号矢

* 收稿日期: 2004-09-11

作者简介: 李海峰 (1980 年生), 男, 硕士研究生; E-mail: lhfvip_2000@163.com

量。

ICA 的目的就是寻求一线性变换 W ，通过它可由观测信号恢复相互独立的源信号

$$Y = WX = WAS \tag{3}$$

$Y = [y_1, y_2, \cdots, y_m]^T$ 是源信号的 $S = [s_1, s_2, \cdots, s_n]^T$ 的估计。所谓估计是指 $Y = \Xi PS$ ，其中 Ξ 是一个实对角阵， P 为一个交换矩阵，也就是说 $Y = [y_1, y_2, \cdots, y_m]^T$ 相对于 $S = [s_1, s_2, \cdots, s_n]^T$ 只是改变了幅值和各分量的排列顺序^[4]。

对于该模型，如果没有关于源信号和混合矩阵的任何先验知识仅从观测信号恢复出源信号是不可能的。所以，一般作如下假设^[5]：①源信号各分量之间相互统计独立；②观测信号的数目大于或等于源信号的数目；③源信号中至多有一个高斯信号；④混合矩阵是列满秩的。

ICA 的通用方法包括：①数据的预处理；②非高斯性度量的定义；③目标函数的优化。目标函数值的大小表示了输出 $Y = [y_1, y_2, \cdots, y_m]^T$ 各分量之间的独立程度。通过梯度法等方法迭代更新分离阵 W ，使目标函数值达到最优，进而使输出 Y 各分量尽可能相互独立。选择不同的目标函数，就得到不同的 ICA 算法，如最小互信息法、最大熵法等。本文采用文献 [5] 提出的快速固定点算法 (FastICA)。

2 水印系统算法

2.1 水印信号预处理

本文采用二值图像作为水印信号。优点之一就是提取出的水印直观，不需再利用原水印信号进行相关性计算，可以直接使用它对载体中是否含有水印进行判别。另外，由于提取出的水印总能包含一定程度的可辨识的结构信息，因此，采用二值图像作为水印信号对于攻击有更强的鲁棒性。

若直接使用水印嵌入，则保密性差。如果攻击者从载体数据中获得了水印数据，就可以直接了解水印内容，对水印的攻击就很容易了。

本文采用 Arnold 变换^[6]对水印图像进行预处理，如图 1 所示。Arnold 变换描述如下：

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \tag{4}$$

其中， $(x, y)^T, (x', y')^T$ 分别为原图像和变换后的图像的像素位置。

Arnold 变换破坏了水印图像的相关性。置乱后的水印信号看似杂乱无章，即使水印攻击者可以获得水印数据，但他得到的是无任何意义的乱码，攻

击者无法确定是否得到了真正的水印，从而在一定程度上防止了对水印系统的攻击。

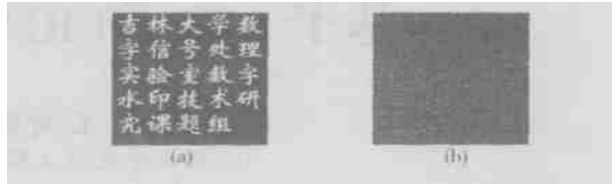


图 1 (a) 置乱前的水印信号; (b) 置乱后的水印信号

Fig 1 (a) Watermark signal before Arnold transform;

(b) Watermark signal after Arnold transform

2.2 水印嵌入算法

本文的水印嵌入算法，充分利用了 SVD 的性质。假设载体图像 I 为大小 $N \times N$ 的矩阵 ($I \in C^{N \times N}$)。

步骤 1：对载体图像 I 进行奇异值分解

$$I = USV^H \tag{5}$$

步骤 2：计算水印的嵌入强度 α 。令 $\lambda_{\max}^I, \lambda_{\max}^W$

分别表示载体图像和水印图像 W 的最大奇异值

$$\alpha = c \cdot \frac{\lambda_{\max}^I}{\lambda_{\max}^W} \tag{6}$$

通过实验的方法，在保证不可感知性的情况下，选 $c=5$ 。

步骤 3：将水印信号 W 叠加在载体图像 I 上，然后对之进行奇异值分解

$$I + \alpha \cdot W = U_w S_w V_w^H \tag{7}$$

步骤 4：通过 U, S_w 和 V^H 获得嵌入水印的图像 I^W

$$I_w = US_w V^H \tag{8}$$

由于酉矩阵对 U 和 V^H 代表载体图像的几何特性，因此，已嵌水印图像 I_w 与载体图像 I 几乎完全相同。

步骤 5：生成密钥图像 K 。选用一维 Logistic 映射^[7]产生混沌序列，并截短为 $L = N \times N$ ，其中 N 载体图像的宽度。将一维序列组合成大小为 $N \times N$ 的二维矩阵 K 。

由于混沌序列具有初值敏感性，因此能保证密钥图像 K 的惟一性。此外，混沌序列具有很弱的互相关性，能使载体图像 I 、水印图像 W 和密钥图像 K 之间尽可能保持独立性，从而有利于提高水印提取的准确度。

步骤 6：生成载体图像 I 的一个拷贝 I_k ，用于鉴别图像的所有权。

$$I_k = I + \beta \cdot K \tag{9}$$

其中， β 是一个控制密钥嵌入强度的大于零的常数。

2.3 水印提取算法

ICA 处理是水印提取算法的核心。如前文所述, ICA 通常要求观测信号数目不小于源信号数目。因此, 就本文算法而言, 至少需要载体图像、水印图像和密钥图像的 3 个线性混合信号。水印提取算法步骤如下:

步骤 1: 对可能已遭受恶意或非恶意攻击的已嵌水印图像 I'_w 进行奇异值分解

$$I'_w = U'S'_{w}V'^H \tag{10}$$

步骤 2: 第一个观测信号 D_1 由下式计算得到

$$D_1 = U_wS'_{w}V'^H_w \tag{11}$$

步骤 3: 第 2 个观测信号 D_2 与载体图像的拷贝 I_k 完全相同

$$D_2 = I_k \tag{12}$$

步骤 4: 利用密钥图像 K 和观测信号 D_1 、 D_2 , 第 3 个混合信号 D_3 可由下式得到:

$$D_3 = D_2 + \gamma_1 \circ K + \gamma_2 \circ D_1 \tag{13}$$

其中, γ_1 、 γ_2 是任意实数。简单起见, 置 γ_2 为 0。

在方程 (11)、(12)、(13) 中, D_1 、 D_2 和 D_3 都是载体图像 I 、水印图像 W 和密钥图像 K 的线性叠加。因此, 重写上式如下:

$$D_1 = m_{11} I + m_{12} W + m_{13} K \tag{14}$$

$$D_2 = m_{21} I + m_{22} W + m_{23} K \tag{15}$$

$$D_3 = m_{31} I + m_{32} W + m_{33} K \tag{16}$$

其中, $m_{i,j} (i = 1, 2, 3; j = 1, 2, 3)$ 是未知混合系数。只要系数矩阵

$$Q = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix}$$

满足列满秩, 水印信号 W 就能通过对混合信号 D_1 、 D_2 和 D_3 进行 ICA 提取出来。

步骤 5: 对观测信号 D_1 、 D_2 和 D_3 进行预处理。首先使观测信号为零均值信号, 然后对零均值信号进行白化 (各分量不相关, 且方差为 1)。

步骤 6: 对预处理后的观测信号进行独立分量分析。本文采用 FastICA 算法^[5]。该算法基于负熵最大化, 其目标函数为:

$$J(y) \propto [E\{G(y)\} - E\{G(v)\}]^2 \tag{17}$$

式中, $G(\cdot)$ 为任意非二次型函数。本算法选 $G(u) = \frac{1}{4}u^4$ 。 v 是一零均值单位方差的高斯变量。

步骤 7: 根据水印预处理过程中相关参数, 对由步骤 6 提取出的水印图像进行逆置乱, 从而恢复出水印信号 W 。

3 对比实验及讨论

本文实验采用 $256 \times 256 \times 8$ bit 的灰度图像作为载体图像。 256×256 的二值图像作为水印信号。相同大小的密钥图像 (图 2 (c)) 由一维混沌序列映射生成。

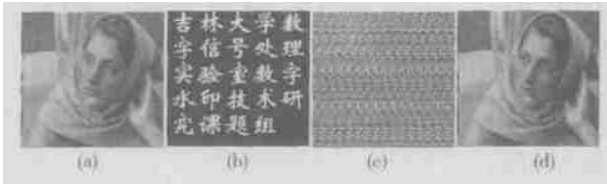


图 2 (a) 载体图像; (b) 水印信号; (c) 密钥图像; (d) 已嵌水印的图像

Fig. 2 (a) Cover image; (b) Watermark; (c) Key image; (d) Marked image

3.1 不可感知性

主观上, 不可感知性可由人眼进行判断。采用 Barbara 作为载体图像, 水印嵌入前后分别如图 2 (a) 和图 2(d) 所示。主观上察觉不到由于嵌入水印所造成的图像降质。

客观上, 不可感知性由载体图像与嵌入水印图像之间的峰值信噪比 (PSNR) 来评估。

$$PSNR = 10 \log \frac{M \times N \times 255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I(i, j) - I_w(i, j))^2} \tag{18}$$

其中, $I(i, j)$ 、 $I_w(i, j)$ 分别是载体图像和已嵌入水印的图像。显然, PSNR 值越大, 不可感知性越好。

当载体图像分别为 Lena、Peppers、Boat 和 Barbara 时, 实验数据如表 1 所示。由表中数据可知, 水印的嵌入强度由载体图像、水印图像的性质 ($\lambda_{\max}^I \setminus \lambda_{\max}^W$) 共同决定, 因此算法具有一定的自适应性。同时, 不可感知性得到了很好的保证。故本文提出的基于 SVD 和 ICA 的水印算法在水印嵌入容量与不可感知性之间取得了很好的折中。

表 1 不可感知性比较

Tab 1 The imperceptibilities for different images			
测试图像	嵌入强度	PSNR/dB	$\lambda_{\max}^I \setminus \lambda_{\max}^W$
Lena	10.2144	41.5446	2.0431
Peppers	11.3920	40.4049	2.2761
Boat	13.3120	39.3511	2.6634
Barbara	10.7776	40.6819	2.1577

3.2 系统鲁棒性

鲁棒性是本文算法追求的另一个目标。通常采用归一化相关系数 (NC) 来衡量提取的水印与原

始水印之间的相似程度。

$$NC = \frac{\sum_{i=1}^P \sum_{j=1}^Q [W(i,j) W'(i,j)]}{\sum_{i=1}^P \sum_{j=1}^Q [W(i,j)]^2} \tag{19}$$

其中, $W(i,j)$ 、 $W'(i,j)$ 分别是原始水印和提取的水印。显然, $NC(0 \leq NC \leq 1)$ 越大, 二者的越相似。

以下是本文 SVD-ICA 算法与 Dan Yu 算法^[3] 的对比实验结果, 前提是不可感知性 (用 PSNR 度量) 相同。

3.2.1 针对信号处理的鲁棒性 图像的传输过程中不可避免的要受到噪声的干扰。水印信号会被噪声影响, 甚至部分信号相互叠加、相关, 最终导致水印信号失效。图 3 (a) 给出了噪声为高斯噪声时的检测曲线。由于 Dan Yu 算法^[3] 为空域水印算法, 而且水印的嵌入强度受到不可感知性的限制, 因此, Dan Yu 算法对于噪声很敏感。

维纳滤波也是常见的图像处理操作之一。窗口尺寸越大, 图像降质越大, 水印信号遭受的破坏也越强。窗口为 9×9 时, 嵌入水印的图像的商业价值受到了影响, 而此时 SVD-ICA 算法的 NC 为 0.3852, 可以清楚地辨认水印 (图 3b)。

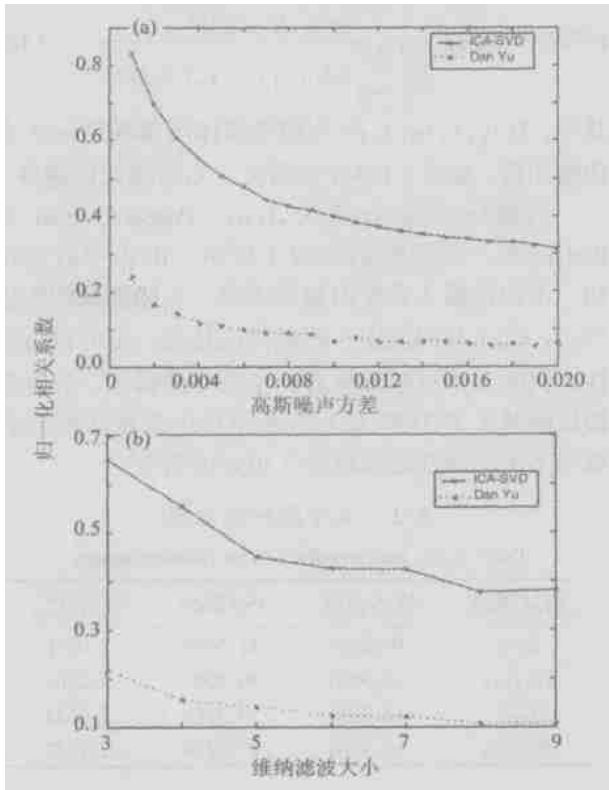


图 3 (a) 高斯噪声; (b) 维纳滤波
Fig 3 (a) Gaussian noise; (b) Wiener filter

3.2.2 针对几何操作的鲁棒性 水印如何对抗几何攻击是一个极具挑战性的课题。

先将图像进行比例缩小, 然后在比例放大到原始大小, 这一过程属于有损过程, 图像和水印信息都有不同程度的损失。图 4 (a) 给出了不同伸缩因子下水印的检测结果。由实验数据可知, SVD-ICA 算法优于 Dan Yu 算法^[3]。

图 4 (b) 给出了旋转加剪切情况下水印检测性能曲线。当旋转角度从 0°到 90°变化时, SVD-ICA 算法的检测性能曲线关于 45°具有一定的对称特性, 优于 Dan Yu 算法^[3]。

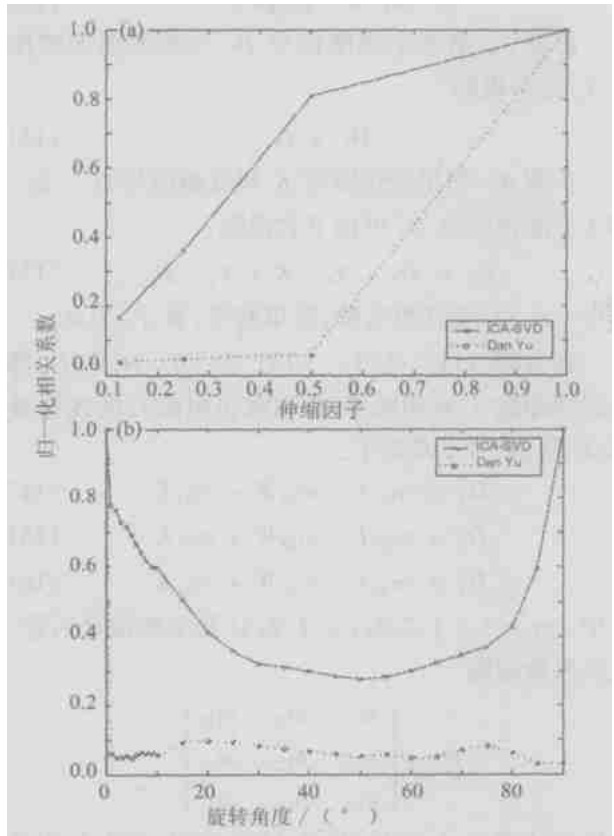


图 4 (a) 伸缩攻击; (b) 旋转攻击
Fig 4 (a) Scale attack; (b) Rotation attack

4 总 结

本文提出了一种基于 SVD 和 ICA 的鲁棒水印算法。SVD 应用于水印的嵌入过程, ICA 应用于水印的提取。该水印系统具有如下特点:

- (1) 水印信号经 Arnold 变换预处理, 提高了水印系统的安全性。
- (2) 水印的嵌入强度由载体图像、水印图像的性质 ($\lambda_{\max}^I \setminus \lambda_{\max}^W$) 共同决定, 因此 SVD-ICA 算法具有一定的自适应性。

(3) SVD-ICA 水印算法具有较全面的鲁棒性。尤其对于几何攻击，如伸缩、旋转、剪切等。

参考文献：

[1] 杨义先, 纽心忻, 任金强. 信息安全新技术[M] . 北京: 北京邮电大学出版社, 2002.

[2] BARNI M, BARTOLINI F, PIVA A. Improved wavelet-based watermarking through pixel-wise masking[J] . IEEE Trans Image Processing, 2001, 10(5): 783—791.

[3] YU D, SATTAR F, MA K K. Watermark detection and extraction using independent component analysis method[J] . Eurasip J Applied Signal Processing, 2002(1): 92—104.

[4] 李木森, 毛剑琴. 盲信号分离的现状和展望[J] . 信息与电子工程, 2003, 1(1): 69—79.

[5] HYVARINEN A, OJA E. Independent component analysis: algorithms and applications[J] . Neural Networks, 2000 (13): 411—430.

[6] 赵慧. N 维 Arnold 变换及其周期性[J] . 北方工业大学学报, 2002, 14(1): 21—25.

[7] NIKOLAIDIS ATHANASIO, PITAS. IOANNIS. Comparison of different chaotic maps with application to image watermarking[C] . Proceedings of International Symposium on Circuits and Systems, 2000: 509—512.

A Robust Watermarking Scheme Based on SVD and ICA

LI Hai feng, WANG Shu xun, WEN Quan, SONG Wei wei

(College of Communication Engineering, Jilin University, Changchun 130025, China)

Abstract: A novel watermarking algorithm for the digital image is proposed. The Singular Value Decomposition (SVD) is employed during the embedding process of the watermarking. Instead of random sequences, some readable signature is used as watermark. By means of Independent Component Analysis (ICA), the watermark is successfully extracted. In the proposed algorithm the capacity of the embedded watermark is enhanced, and at the same time the transparency can be guaranteed. Our method can extract the watermark without taking attacks into consideration. Experiment results have demonstrated that the proposed approach is robust against the common signal processing, such as JPEG compression, additive noise. In particular, it is also robust against geometric attacks, such as rotation, cropping, scaling etc.

Key words: digital watermarking; SVD; ICA; Arnold transform; chaotic sequence