

基于分块奇异值分解的盲水印技术

陈琼 伍祥生 刘飞

(湖南师范大学信息技术系,长沙 410081)

摘要 基于奇异值分解的数字水印方案,具有很强的鲁棒性,但是它也存在着一些不足的地方。为此提出了一种新的基于分块奇异值分解盲水印方法,在图像水印信息经过置乱处理后嵌入到原始载体图像分解所得的首矩阵中。运用置乱方法和奇异值分解方法,提高了水印的不可见性,保证了水印的安全性。在水印的检测与提取过程中不需要原始载体图像,更加利于实际中的应用。实验结果证明,该方法具有较好的不可见性,对常见的图像处理具有良好的鲁棒性。

关键词 奇异值分解 数字图像水印 Arnold变换 盲水印

中图分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2007)09-1558-04

A Blind Watermarking Based on Block—SVD

CHEN Qiong, WU Xiang-sheng, LIU Fei

(The Department of Information Technology, Hunan Normal University, Changsha 410081)

Abstract The existing watermarking based on SVD (singular value decomposition) is robust, but still there are some defects. In this paper, we present a new blind watermarking method based on block—SVD. The Watermarking is embedded into the unitary matrices which are obtained using the singular value decomposition of the source image according to the relationships between the coefficients of the unitary matrices. The implementation of the scrambling encryption and singular value decomposition methods provides the invisibility and the security of the watermark. This method is not needed the source image during the detection and extraction so that it could be better applied into the practice. Experiments demonstrate that the proposed scheme is invisible and robust against common image processing.

Keywords singular value decomposition, digital image watermarking, arnold transformation, blind watermarking

1 引言

随着计算机技术和多媒体技术的飞速发展,数字化多媒体信息产品的传播和交易变得越来越便捷。在网络传输逐渐成为人们之间信息交流的重要手段的同时,信息安全问题也日益显露出来。信息隐藏技术比较好地解决了传统密码技术的一些问题,其在计算机多媒体领域的重要应用——数字水印技术为保护多媒体信息的版权和保证多媒体信息的安全使用提供了一种很有效的手段。变换域数字

水印算法具有很好的鲁棒性,且其嵌入的水印能量可以分布到空域的所有像素上,同时可与国际数据压缩标准兼容。目前的变换域数字水印技术大多数是基于离散余弦变换(DCT)、傅里叶变换(FFT)、小波变换(DWT)的,也有一些是基于人的视觉特征的。中国科学院自动化研究所所长谭铁牛教授曾在文献[1]中提出了一种基于奇异值分解的数字水印方案,将水印嵌入到分解所得的奇异值对角阵中,此方法具有很强的鲁棒性。后来的一些研究也在此基础上进一步发展,但是它也存在着一些不足的地方,例如矩阵运算量大,导致大图像嵌入水印的时间

基金项目:湖南省教育厅项目(04C204)

收稿日期:2006-03-30;改回日期:2006-05-31

第一作者简介:陈琼(1981~),女,湖南师范大学计算机软件与理论专业硕士研究生。研究方向为图像处理和数字水印。E-mail: wxs

@hunnu.edu.cn

较长,且在使用工具计算时的误差可能会引起水印图像在对角线方向上有一定的失真。

本文提出了一种新的基于分块奇异值分解盲水印方法,在图像水印信息经过置乱处理后嵌入到原始载体分解所得的首矩阵中。运用置乱方法和奇异值分解,提高了水印的不可见性,保证了水印的安全性。在水印的检测与提取过程中不需要原始载体图像,更加利于实际中的应用。实验结果证明,该方法具有较好的不可见性,对常见的图像处理具有良好的鲁棒性。

2 2维 Arnold 变换和基于奇异值分解的水印技术

在介绍我们的方案之前,先回顾一下基础理论。

2.1 2维 Arnold 变换^[2]

2维 Arnold 变换也就是通常所说的 Arnold 变换,它是在遍历理论研究中提出的一种取模形式的非线性变换,俗称猫脸变换(cat mapping)。其变换矩阵如下:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1 \quad (1)$$

从变换矩阵可知,这种变换实际上是一种点的位置的移动,且可以一直迭代下去。对数字图像来说,可以看成是函数在离散网格中的采样,从而得到一个表示图像的矩阵。对于 $N \times N$ 的数字图像,离散化的 Arnold 变换矩阵如下:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \quad (2)$$

如要变换的矩阵为 A ,反复进行这一变换,则有迭代公式:

$$P_{ij}^{n+1} = AP_{ij}^n \pmod{N}, n = 0, 1, 2, 3, \dots \quad (3)$$

其中, $P_{ij}^n \in [0, N-1] \times [0, N-1]$, $P_{ij}^0 = (x, y)$ 为迭代第 n 步时点的位置。一次次的迭代会使图像变得“杂乱无章”,但继续使用该变换将会出现一幅与原图像相同的图像,从而达到图像传输过程中的隐蔽效果。Dyson 和 Falk 分析了离散 Arnold 变换的周期性,给出了对于任意的 $N > 2$ 的图像,Arnold 变换的周期 $T \leq N^2/2$ 。

2.2 矩阵的奇异值分解

一幅灰度图像从线性代数的角度来看,是一个具有非负值的矩阵。假定这幅灰度图像用字母 I 来表示, $I \in \mathbf{R}^{N \times N}$, \mathbf{R} 表示实数域。那么 I 的奇异值分

解定义为

$$I = USV^T \quad (4)$$

其中, $U, V \in \mathbf{R}^{N \times N}$ 两者都是酉矩阵, $S \in \mathbf{R}^{N \times N}$ 是对角阵。

2.3 传统的基于奇异值分解的数字水印方法^[1]

在数字图像处理中,运用奇异值分解技术主要有以下几个方面的优势^[1]:第一, SVD 分解对所要进行变换的矩阵的大小没有什么限制,可以是方阵也可以是长矩阵;第二,对于一般的图像处理,奇异值的稳健性非常好,不会有很大的变化;第三,奇异值反映的是图像内蕴特性而不是视觉特性,反映的是图像矩阵元素之间的关系。

传统的 SVD 方法嵌入水印过程描述如下:

(1) 将图像矩阵进行 SVD 分解:

$$[U \ S \ V] = \text{SVD}(A) \quad (5)$$

(2) 水印 W 被叠加到矩阵 S 中,并对新产生的矩阵进行 SVD:

$$S + \alpha W \Rightarrow U_1 S_1 V_1^T \quad (6)$$

(3) 重构图像得到含有水印的图像 I' :

$$I' \Leftarrow U S_1 V_1^T \quad (7)$$

在水印的检测过程中,如果给定 U_1, S, V_1 和可能损坏的含水印图像 I^* ,那么就可以提取出可能已经失真的水印 W^* ,即

$$I^* \Rightarrow U^* S_1^* V_1^{*T} \quad (8)$$

$$D^* \Leftarrow U_1 S_1^* V_1^T \quad (9)$$

$$W^* \Leftarrow \frac{1}{\alpha} (D^* - S) \quad (10)$$

3 新的基于奇异值分解的盲水印技术

3.1 水印嵌入的算法

在最近基于奇异值分解的数字水印文献[1]、[3]中,大多都将水印嵌入到分解后的对角矩阵 S 中,这是利用了 S 的系数在一般的图像处理中具有较好的鲁棒性的特点。但是,由于 S 是一个对角阵,提供的被用来嵌入水印的系数个数不多,另外, S 系数的修改也可能引起较大的图像降质。而通常情况下,对于一个基于分块的奇异值分解技术来讲,矩阵 U 里的一些系数之间的关系在多数的图像处理中是能够较稳定的保持下来的。因此,本文中用的是矩阵 U 的这一个特征来嵌入水印。

以一幅 $N \times N$ 的灰度图像和 $w \times w$ 的二值水印图像为例(当然,其他的长矩阵也可以用类似的方

法来处理)。设原始图像为 I , 水印为 W 。本文算法的基本思想就是先将水印图像置乱加密, 再将载体图像分成互不重叠的 $m \times m$ ($m=8$) 大小的块, 随机的选择适当多的分块分别进行 SVD 后, 再嵌入处理好的水印信息, 反变换后即可得到含水印的图像。该方法是对分块进行 SVD 而不是对整个图像块, 所以缩短了嵌入和提取水印的时间, 这对于大图像来说效果尤其明显。

水印嵌入算法描述如下:

(1) 对水印图像 W 进行预处理。利用 Arnold 图像置乱技术给水印加密, 迭代的次数 k_1 就是一个密钥。

(2) 将原始图像 I 分成 $m \times m$ 大小的块, 用密钥 k_2 产生一个随机序列用来选择足够多个子块来嵌入水印信息。

(3) 对所选择的子块 $D\{i, j\}$ 进行 SVD 分解, 即 $[U \ S \ V] = \text{SVD}(D\{i, j\})$ 。

(4) 根据水印信息来修改矩阵的系数值。取出分解所得矩阵 U 并求出 U 矩阵的相邻元素 U_1, U_2 间的幅度之差 d ; 如果幅度差值的正负与嵌入的水印信息匹配则系数不变, 否则就修改系数。

为了保证图像的质量并使水印算法具有更强的鲁棒性, U 的系数还可进行进一步修改。我们增加一个门限值 dT 作为相邻系数间的最小幅度差。修改系数具体过程如下:

如果差值与水印位的正负关系匹配且其差值的幅度小于 dT , 则按如下公式修改系数:

$$U_1 = \text{sgn}(U_1) \times \text{abs}(\text{abs}(U_1) + \text{sgn}(d) \times (dT - \dots \text{abs}(d))/2) \quad (11)$$

$$U_2 = \text{sgn}(U_2) \times \text{abs}(\text{abs}(U_2) - \text{sgn}(d) \times (dT - \dots \text{abs}(d))/2) \quad (12)$$

如果不匹配, 则

$$U_1 = \text{sgn}(U_1) \times \text{abs}(\text{abs}(U_1) - \text{sgn}(d) \times (dT + \dots \text{abs}(d))/2) \quad (13)$$

$$U_2 = \text{sgn}(U_2) \times \text{abs}(\text{abs}(U_2) + \text{sgn}(d) \times (dT + \dots \text{abs}(d))/2) \quad (14)$$

其中, $\text{sgn}(\cdot)$ 为符号函数, $\text{abs}(\cdot)$ 为取绝对值的函数, ‘ \dots ’ 表示续行。

(5) 循环第 3 步至第 4 步直到水印全部嵌入到原始图像中, 用奇异值反变换重构图像 I' , 它就是嵌入水印后的图像了。

3.2 水印的提取算法

水印的提取算法和水印的嵌入算法是对称的。

(1) 可能损坏的含水印图像 I' 分成 $m \times m$ 大小的块, 利用密钥 k_2 产生随机序列来检测出嵌入了水印的子块 $D^*\{i, j\}$ 。

(2) 对每一个子块 $D^*\{i, j\}$ 进行 SVD 分解, 得到 $U^*\{i, j\}$ 、 $S^*\{i, j\}$ 、 $V^*\{i, j\}$, 计算出 $U^*\{i, j\}$ 的相邻元素之间的关系, 来判断嵌入的水印信息。

(3) 利用 Arnold 反置乱技术和提供的密钥 k_1 解密提取出来的信息, 即得到可能已经失真的水印 W^* 。

4 实验结果

实验中采用了 256×256 的“Lena”图像作为原始载体图像 I , 用 32×32 大小的二值图像“湖南师大”作为水印 W , 并使用 Matlab 来做仿真实验。原始图像 I 和嵌入了水印后的图像 I' 之间的相似程度, 我们采用峰值信噪比 PSNR (Peak Single-to-Noise Ratio) 来衡量^[4], 它的值越大表示图像 I' 的保真度越好, 也就是说两个图像越相象。提取出的水印图像 W^* 和原始水印图像 W 之间的相似性, 使用专门针对二值图像水印的相似性测量标准^[5], 用 NC 值来表示, 它的值越大表示两个图像 W 和 W^* 越相象。PSNR 和 NC 的定义如下:

$$\text{PSNR} = M \times N \max_{m,n} (I_{m,n}^2) / \sum_{m,n} (I_{m,n} - I'_{m,n})^2 \quad (15)$$

$$\text{NC} = \sum_{m,n} (W_{m,n}^* \oplus \sim W_{m,n}) / (m * n) \quad (16)$$

其中, ‘ \oplus ’ 表示异或运算, ‘ \sim ’ 表示逻辑非运算。

如图 1(a) 为原始图像 Lena, 图 1(b) 为采用本文算法嵌入水印后的图像, PSNR 值为 47.1761 dB。图 1(c) 为原始水印图像, 图 1(d) 为对含水印的图像进行质量因子为 70 的 JPEG 压缩后所提取的水印图像, 与原始水印的相关系数值 $\text{NC} = 0.9590$ 。图 1(e) 为含水印图像在 0.03 的高斯噪声的影响下所提取的水印, $\text{NC} = 0.9834$ 。图 1(f) 为 0.02 的椒盐噪声干扰后所提取的水印图像, $\text{NC} = 0.9238$ 。图 1(g) 为含水印图像经过中值滤波后所提取出来的水印图像, $\text{NC} = 0.9600$ 。图 1(h) 为在图像上裁剪了大小为 129×114 的小块后所提取的水印图像, $\text{NC} = 0.8252$ 。

我们也尝试了多个不同的图像进行该实验, 实验结果表明, 本文所提出的这种新的基于奇异值分解的数字图像水印方案非常鲁棒。限于篇幅, 只给出了以上的实验结果。在实际的应用中, 水印算



(a) Lena 原图



(b) 嵌入水印后的图像 PSNR = 47.1761



(c) 原始水印图像



(d) JPEG 压缩后
提取的水印,
NC = 0.9590



(e) 经过高斯噪声后
提取的水印,
NC = 0.9834



(f) 经过椒盐噪声后
提取的水印,
NC = 0.9238



(g) 中值滤波后
提取的水印,
NC = 0.9600



(h) 剪切攻击后
提取的水印,
NC = 0.8252

图1 仿真实验中的不同图像

Fig.1 The different images in simulated experiments

法的好坏不仅要看水印是否鲁棒,还要看水印嵌入的时间。本文提出的基于分块的奇异值分解方法明显比以往的奇异值分解方法具有更快的速度,尤其对于大图像来说,节省了不少的运行时间。且提取和检测水印时,不需要原始图像只需要原始水印和加密密钥就可以完成工作,即是一种盲水印算法,在实际中具有很大的应用潜力。

5 结 论

本文提出了一种新颖的基于奇异值分解的盲数字水印技术。它有别于通常研究的 DCT, DFT 和 DWT 变换的一种变换域方法,是非常鲁棒的。分块思想的运用使得计算的速度大大增快,特别是在提取和检测水印时,不需要原始图像就可以完成工作,是一种盲水印算法。仿真实验证明,该算法非常有效,很好的满足了数字水印的透明性和鲁棒性,能经受住通常的图像处理操作且具有很大的应用潜力。

参考文献 (References)

- LIU Rui-zhen, Tan Tie-niu. SVD based digital watermarking method [J]. Chinese Journal of Electronics, 2001, 29(2): 168 ~ 171. [刘瑞贞, 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.]
- Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling technology based on arnold transformation [J]. Journal of Computer-Aided Design & Computer Graphics, 2001, 13(4): 338 ~ 341. [丁伟, 闫伟奇, 齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报, 2001, 13(4): 338 ~ 341.]
- Sun R, Sun H, Yao T. A SVD and quantization based semi-fragile watermarking technique for image authentication [A]. In: Proc. Internet. Conf. Signal Process [C], 2002, 2: 1952 ~ 1955.
- Sun Sheng-he, Lu Zhe-ming, Niu Xia-mu. The Technology and Application of Digital Watermarking [M]. Beijing: Science Press, 2004: 510 ~ 512. [孙圣和, 陆哲明, 牛夏牧. 数字水印技术及应用[M]. 北京: 科学出版社, 2004: 510 ~ 512.]
- Yang Hen-fu, Chen Xiao-wei. A robust image-adaptive public watermarking technique in wavelet domain [J]. Journal of Software, 2003, 14(9): 1652 ~ 1660. [杨恒伏, 陈孝威. 小波域鲁棒自适应公开水印技术[J]. 软件学报, 2003, 14(9): 1652 ~ 1660.]