

一种 NMF 和 SVD 相结合的鲁棒水印算法

刘如京 王 玲

(湖南大学电气与信息工程学院 长沙 410082)

摘 要 提出了一种非负矩阵变换(NMF)和奇异值分解(SVD)相结合的数字水印算法。该算法对宿主图像进行离散小波变换,然后选取低频部分进行非负矩阵变换和奇异值分解,最后在奇异值中嵌入 Arnold 置乱后的水印。实验表明,该算法在获得良好的视觉效果的同时,又具有很好的鲁棒性,对加噪、滤波、剪切等图像攻击有很好的抵抗能力。

关键词 离散小波变换,非负矩阵变换,奇异值分解,Arnold 置乱

中图分类号 TP391

文献标识码 A

Robust Watermarking Scheme Based on NMF and SVD

LIU Ru-jing WANG Ling

(College of Electrical and Information Engineering, Hunan University, Changsha 410082, China)

Abstract In this paper, a digital watermarking algorithm based on nonnegative matrix factorization(NMF) and singular value decomposition(SVD) was proposed. The host image was decomposed with DWT. NMF and SVD were applied to the low frequency component of the original image. The watermark after Arnold scrambling was embedded into the singular value of the image. The experiment results indicate that the proposed scheme can obtain better visual effect and it is robust against attacks such as added noise, filtering and cropping.

Keywords DWT, NMF, SVD, Arnold scrambling

1 引言

数字水印是一种新型实用的信息隐藏和版权保护技术,近年来已经引起了极大的关注并得到迅速发展。数字水印算法归纳起来大致可以分为空域和变换域两种。变换域方法已成为数字水印算法研究的主流,其中数字小波变换(DWT)域的水印技术因其具有良好的多分辨率表示、时频局部分析等特性,且易于兼容 JPEG2000、MPEG-4 压缩标准等特点,得到了普遍关注。

NMF^[1](Nonnegative Matrix Factorization)是 Daniel D Lee 等在 1999 年“Nature”中首先提出的算法,该算法对一个非负的矩阵进行分解,得到两个非负的矩阵。自从 Lee 等提出了 NMF 的简单算法后, NMF 一直不断地完善和发展着,已经成功应用于人脸识别、图像散列、音乐信号的分析分离、图像融合等领域。近几年也有人提出将 NMF 应用到数字水印技术中。文献[2]中牛万红等人设计了一种基于 NMF 构造密钥的二值零水印算法,但是该算法对噪声和滤波等攻击的抵抗力不佳。文献[3]中 Wei Sun 等人在小波域中将 NMF 应用在数字水印技术中,并运用支持向量机(SVMs)对图像的特征进行分类,计算量大,最后的水印不可见性和鲁棒性并不是很理想。本文提出了一种将 NMF 应用到 DWT 域的水印算法,并且在 NMF 变换后又进行了 SVD(Singular Value Decomposition)变换,使得水印具有更好的鲁棒性。奇异值分解(SVD)是一种将矩阵对角化的数值技术,从图像处理的角度看,奇异值对应于图像的亮度特性,奇异向量表征了图像的几何特性,图像奇异值的稳定性非常好,在图像被施加小的扰动时奇异值不会有大的变化,并且在水印嵌入宿主图像之前将水印进行 Arnold 置乱,以提高水印图像的安全性。本文算法经过试验测试,对于常见的图像攻击具有很好的鲁棒性。

2 水印算法的思想

2.1 小波变换

小波变换是一种多尺度信号分析方法,近几年受到广泛关注。它克服了傅里叶变换固定分辨率的弱点,既可分析信号概貌,又可分析信号的细节。小波变换用于图像处理是小波变换应用效果比较突出的领域之一。其基本思想就是把数字图像多分辨率地分解成不同空间、不同频率的子图像,然后根据各个子图像的特点有针对性地进行处理。每一级分解都把图像分解为 4 个频带:水平(HL)、垂直(LH)、对角(HH)和低频(LL),其中低频(LL)部分还可以进行下一级的分解,从而构成了小波的塔式分解。一幅图像经过分解之后,图像的能量主要集中于低频部分,这也是视觉重要部分;而图像的高频部分即图像的细节部分所含能量较少,分布在 HL, LH, HH 3 个子图中,主要包含了原图的边缘和纹理部分信息。

2.2 非负矩阵变换

NMF^[1,4]是目前国际上一种新的矩阵分解方法。NMF 问题可描述为:已知一个非负矩阵 V ,要找出非负的 $n \times r$ 矩

到稿日期:2010-03-26 返修日期:2010-06-27 本文受湖南省教育厅资助科研项目(06C522)资助。

刘如京(1984—),女,硕士生,主要研究方向为图形图像处理,E-mail:liurujing_hnu@163.com;王 玲(1962—),女,博士,教授,博士生导师,主要研究方向为现代通信技术及图像处理。

阵 W 和非负的 $r \times m$ 矩阵 H , 使 $V = W \cdot H$, 其中 r 须事先给定, 通常 r 应小于 m 和 n 。该算法是在 W 和 H 是非负矩阵的约束条件下使目标函数 $|V - W \times H|^2 = \sum_{i,j} (V_{i,j} - (W \times H)_{i,j})^2$ 取极小。将目标函数分别对 W 和 H 求导数, 并取迭代步长为 $\eta_{i,j} = H_{i,j} / (WW^T H)_{i,j}$, ($i=1, 2, \dots, n; j=1, 2, \dots, m$), 由梯度下降法就可以得到 NMF 算法的迭代公式:

$$\begin{aligned} H_{i,j} &\leftarrow H_{i,j} \frac{(W^T V)_{i,j}}{(W^T W H)_{i,j}} \\ W_{i,j} &\leftarrow W_{i,j} \frac{(V H^T)_{i,j}}{(W H H^T)_{i,j}} \\ (i=1, 2, \dots, n; j=1, 2, \dots, m) \end{aligned}$$

上式中的更新规则已被证明是收敛的。在算法中, 只用了乘法运算, 保证了结果的非负性。

由上述可知, NMF 是用非负性约束来获取数据表示的一种方法。非负性是对矩阵分解非常有效的条件限制, 它导致了对于原始数据的基于部分的表示形式, 即样本数据只允许加性的和非负的组合。算法所得到的非负基向量组 W 具有一定的线性无关性和稀疏性, 从而使得其对原始数据的特征及结构具有相当的表达能力, 使得该算法具有很强的应用背景。同时非负性的条件限制符合许多实际问题的要求, 例如, 在图像处理中, 图像像素的灰度值总是非负的, 而正的混合也使得混合图像的像素灰度值是非负的, 即分解算法得到的结果能直接表达一定的物理意义。

2.3 奇异值分解

从线性代数的角度看^[9], 一幅数字图像可以看成是由许多非负标量组成的一个矩阵。用 $A \in R^{M \times N}$ 来表示一个图像矩阵, 其中 R 表示实数域。不失一般性, A 可以表示成:

$$A = U \Sigma V^T$$

式中, $U \in R^{M \times N}$ 和 $V \in R^{M \times N}$ 都是正交矩阵, 称为左右奇异阵列, $\Sigma \in R^{M \times N}$ 是一个非对角线上的项都是 0 的矩阵, 其对角线上的元素满足:

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_r > \sigma_{r+1} = \dots = \sigma_M = 0$$

式中, r 是 A 的秩, 它等于非零奇异值的个数, 于是有:

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sigma_M \end{bmatrix}$$

σ_i 是由该分解所唯一确定的, 叫做 A 的奇异值。它是 AA^T 特征值的平方根。分解式 $U \Sigma V^T$ 称作 A 的奇异值分解。

如果 A 是一幅图片, 轻微改变图像的奇异值并不会影响图像的质量, 而且图像受到攻击后奇异值也不会发生很大改变, 因此可以利用奇异值的稳定特性, 提高水印的鲁棒性。

2.4 Arnold 置乱

所谓置乱就是利用某种算法将一幅图像各像素的次序打乱, 但像素的总个数不变, 直方图不变。置乱实际上就是图像的加密。与加密保证安全性不同的是, 将置乱的图像作为秘密信息再进行隐藏, 可以很大限度地提高原始信息的鲁棒性。数字图像的置乱是一种可逆变换, 它通过对数字图像的位置或灰度级等做变换来“扰乱”图像, 以此达到在一定程度上迷惑第三者的目的。经过置乱后的图像, 看起来杂乱无章, 如果不知道所使用的置乱变换, 很难恢复出原始图像。

现在主要将置乱技术用于水印信息的预处理。具体做法

是先对原始水印信息进行置乱, 之后将置乱后的水印信息嵌入到原始图像中, 最后对提取出来的水印信息进行反置乱变换。这样做的好处是既可以增强水印信息的保密性, 也使得嵌入水印后的图像对于某些操作, 特别是对于滤波, 加噪声之类攻击的鲁棒性较好。现在用得较多的置乱技术是基于 Arnold 变换、幻方变换、分形 Hilbert 曲线、IFS 模型、Conway 游戏和 Gray 码变换等。

Arnold 变换是 V. J. Arnold 在遍历理论的研究中提出的一类裁剪变换。从采样原理分析, 数字图像可看作是在二维连续的曲面上, 按照某一间隔和某种策略进行采样所得到的一个二维离散点的阵列, 即一个图像矩阵。对一幅大小为 $N \times N$ 的图像进行 Arnold 变换^[6]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$$

$$(x, y \in \{0, 1, 2, \dots, N-1\})$$

式中, (x, y) 是原图像的像素点, (x', y') 是变换后新图像的像素点, N 是图像阶数即图像的大小, 一般考虑正方形图像, k 是属于 $[1, N]$ 的一个整数。记变换矩阵为 A , 由此做迭代程序:

$$I_{xy}^{n+1} = A I_{xy}^n \pmod{N}, I_{xy}^n = (x, y), n=0, 1, 2, \dots$$

式中, n 代表迭代次数。整个迭代过程呈周期性, 即当此图像经过一定周期的迭代后会重现原图像。由此可见, Arnold 变换算法简单、直观且具有周期性。因此, 本文选取 Arnold 变换对水印图像进行预处理, 从而提高了水印图像的安全性和鲁棒性。

3 水印的嵌入和提取

3.1 水印的嵌入

(1) 首先对宿主图像进行 3 级 DWT 变换;

(2) 对低频逼近子图 A 进行 NMF 分解, 得到 $A = W \cdot H$, 变换误差为 $E = A - W \cdot H$; 然后对 W 矩阵进行奇异值分解, 得到 $W = USV^T$;

(3) 对水印图像 x 做 Arnold 置乱, 将置乱后的水印 x^* 嵌入到 S 中, $K = S + \alpha \cdot x^*$, 其中 α 为水印的嵌入强度;

(4) 对 K 再进行奇异值分解, $K = U_1 S_1 V_1^T$, 然后得到嵌入水印的 W^* , $W^* = US_1 V_1^T$;

(5) 合成非负矩阵 $A^* = W^* \cdot H + E$, 然后进行 DWT 反变换, 得到嵌入水印后的宿主图像。

3.2 水印的提取

水印的提取是水印嵌入的逆过程。

(1) 对嵌入水印的宿主图像进行 3 级 DWT 变换;

(2) 对低频部分 A' 进行 NMF 分解, 得到 $A' = W' \cdot H'$, 对 W' 进行奇异值分解 $W' = U_2 S_2 V_2^T$, 得到 S_2 ;

(3) 然后合成 $K' = U_1 S_2 V_1^T$, 得到提取的未反置乱的水印 $x' = \frac{1}{\alpha} (K' - S)$;

(4) 将 x' 进行 Arnold 反置乱, 得到水印图像 x_1 。

4 实验结果和分析

4.1 算法仿真

本算法在 Matlab7.5 中进行仿真实验。宿主图像是大小为 512×512 的 Lena 灰度图像, 如图 1 所示。对宿主图像进

行3级DWT变换后,取 64×64 大小的低频子带部分进行NMF分解,其中 $r=64$,得到 64×64 大小的 W 矩阵和 H 矩阵。水印图像采用 64×64 大小的baboon灰度图像,如图2所示。按照上述水印嵌入的步骤将水印图像嵌入到宿主图像中,嵌入强度 $\alpha=0.5$,得到的嵌入水印后的宿主图像如图3所示,最后提取的水印图像如图4所示。



图1 宿主图像



图2 原水印图像



图3 嵌入水印后的图像



图4 提取的水印图像

4.2 抗攻击性能测试

在数字图像处理中,通常采用峰值信噪比(PSNR, Peak Signal-to-Noise Ratio)作为嵌入水印图像的客观评价标准。峰值信噪比虽然被广泛地用作图像质量的客观评价指标,但是它没有考虑人类视觉系统(HVS, human visual system),不能准确度量加入水印后图像的视觉质量。因此,有必要寻求一种更为准确的客观评价指标。结构相似度索引^[7](SSIM, structural similarity index)是一种新颖的用于评价两幅图像相似度的客观指标,是在对通用图像质量索引(the universal image quality index)进行改进的基础上得到的。一般地,信号 u 和 v 的结构相似度索引计算如下:

$$SSIM(u, v) = [l(u, v)]^\delta \cdot [c(u, v)]^\gamma \cdot [s(u, v)]^\lambda$$

式中, $\delta > 0, \gamma > 0, \lambda > 0$ 是用于调整3个分量 $l(u, v), c(u, v)$ 和 $s(u, v)$ 的相对重要性参数。 $l(u, v), c(u, v)$ 和 $s(u, v)$ 分别为亮度比较函数、对比度比较函数和结构比较函数。为简单起见,采用如下的SSIM索引形式:

$$SSIM(u, v) = \frac{(2\mu_u\mu_v + C_1) \cdot (2\sigma_{uv} + C_2)}{(\mu_u^2 + \mu_v^2 + C_1) \cdot (\sigma_u^2 + \sigma_v^2 + C_2)}$$

式中, μ_u, μ_v 和 σ_u, σ_v 是信号 u, v 的均值和标准差。 $\sigma_{uv} = \frac{1}{N-1} \sum_{i=1}^N (u_i - \mu_u) \cdot (v_i - \mu_v)$, $C_i = (R_i D)^2, i=1, 2$, 其中 $R_i \ll 1$ 是数值较小的常数, D 是像素值的动态范围。SSIM索引能捕捉图像的局部统计特征,因此和PSNR相比,SSIM索引更近似符合人眼的生理,更适合作为水印隐蔽性的客观评价指标。本文采用SSIM作为水印不可见性的客观度量。

对于提取水印与原水印的相似性,采用相关系数^[8](NC, Normalized Correlation)作为评价标准。 W 和 W' 分别表示原水印图像和提取的水印图像, M 和 N 为水印大小,则NC计算公式为:

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i, j) W'(i, j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W(i, j)^2} \times \sqrt{\sum_{i=1}^M \sum_{j=1}^N W'(i, j)^2}}$$

在实验过程中没有攻击的情况下,得到的SSIM值为42.5386, NC值为0.9946。现在对嵌入水印后的宿主图像进行各种图像攻击,提取的水印NC值见表1。

表1 攻击后提取的NC值

攻击	NC
高斯噪声 0.03	0.9532
椒盐噪声 0.03	0.9620
乘性噪声 0.03	0.9134
中值滤波 5×5	0.9532
旋转 20°	0.8286
JPEG 压缩 10	0.9412
剪切 1/4	0.7108
图像增亮	0.8612
增加对比度	0.8234

从表1中数据可见,本文算法鲁棒性很好,对常见的图像攻击有很好的抵抗能力。现在改变宿主图像,分别用barbara, cameraman, peppers作为宿主图像进行试验,结果见表2。数据显示的鲁棒性依然比较好。

表2 改变宿主图像后的实验结果

攻击	NC		
	barbara	cameraman	peppers
高斯噪声 0.03	0.9549	0.9198	0.9358
椒盐噪声 0.03	0.9601	0.9097	0.9140
乘性噪声 0.03	0.9404	0.9139	0.9341
中值滤波	0.9322	0.9251	0.9294
旋转	0.8291	0.7887	0.7936
JPEG 压缩	0.9352	0.9108	0.9117
剪切	0.8277	0.7957	0.7985
图像增亮	0.8713	0.8642	0.8795
增加对比度	0.8385	0.8192	0.8346

结束语 本文提出了一种将NMF和SVD相结合的鲁棒水印算法。算法在DWT域实现,NMF和SVD的结合提高了水印的鲁棒性。在评估水印性能时考虑到了人类视觉系统(HVS),采用SSIM索引作为水印隐蔽性的客观度量指标。仿真实验表明,本算法具有很好的水印不可见性和鲁棒性。

参考文献

- [1] Lee D D, Seung H S. Learning the parts of objects by non-negative matrix factorization[J]. Nature, 1999, 401: 788-791
- [2] 牛万红, 潘晨. 一种基于NMF的零水印算法[J]. 济南大学学报: 自然科学版, 2009, 23(3): 270-274
- [3] Sun Wei, Lu Wei. Blind Image Watermarking Analysis Using DWT and Non-negative Matrix Factorization[C]// Chinese Conference Pattern Recognition, 2008 (CCPR08). Beijing, 2008: 1-5
- [4] Lee D D, Seung H S. Algorithms for non-negative matrix factorization[C]// Proceedings of Neural Information Processing Systems. 2001, 13: 556-562
- [5] Aase S O, Husoy J H, Waldemar P. A critique of SVD-based image coding systems[J]. IEEE International Symposium on Circuits and Systems, 1999, 5(4): 13-16
- [6] 吴昱升, 王介生, 刘慎全. 基于Arnold变换的数字图像置乱技术[J]. 计算机辅助与图形学学报, 2001, 13(4): 338-341
- [7] Zhou Wang, Bovik A C, Sheikh H R, et al. Image Quality Assessment: From Error Visibility to Structural Similarity[J]. IEEE Transaction on Image Processing, 2004, 13(4): 600-612
- [8] 金聪, 等. 数字水印理论与技术[M]. 北京: 清华大学出版社, 2008