文章编号:1673-5005(2016)01-0177-06 doi:10.3969/j.issn.1673-5005.2016.01.025

基于 PCA 和 DWT 的强鲁棒数字水印算法

郑秋梅, 张 明, 王风华, 刘 涞

(中国石油大学计算机与通信工程学院,山东青岛 266580)

摘要:针对传统离散小波变换(DWT)数字水印算法抗几何攻击能力较弱的问题,提出一种基于主成分分析(PCA)和 DWT 的新的数字水印算法。新算法对载体图像进行一级小波分解,在低频子带上用主成分分析提取出既含有高频又含有低频成分的主成分系数,将水印嵌入到提取出的主成分系数中。实验结果表明,与传统 DWT 水印算法相比,该算法不仅明显提高了抗剪裁、旋转等抗几何攻击能力,对加噪、图像灰度值变化等攻击也表现出了很强的鲁棒性。

关键词:数字水印; 离散小波变换(DWT); 主成分分析(PCA); 鲁棒性

中图分类号:TP 391 **文献标志码**:A

引用格式:郑秋梅,张明,王风华,等. 基于 PCA 和 DWT 的强鲁棒数字水印算法[J]. 中国石油大学学报(自然科学版),2016,40(1):177-182.

ZHENG Qiumei, ZHANG Ming, WANG Fenghua, et al. Robust digital watermarking algorithm based on PCA and DWT [J]. Journal of China University of Petroleum(Edition of Natural Science), 2016,40(1):177-182.

Robust digital watermarking algorithm based on PCA and DWT

ZHENG Qiumei, ZHANG Ming, WANG Fenghua, LIU Lai

(*College of Computer & Communication Engineering in China University of Petroleum*, *Qingdao* 266580, *China*)

Abstract: The digital watermarking algorithm based on discrete wavelet transform (DWT) is weakly resistant to geometric. This paper presents a digital watermarking algorithm based on principal component analysis and DWT transform. In this algorithm, the host image is first transformed with DWT, and principle component analysis (PCA) is used to de-correlate the image pixel to obtain the principle components. The watermark is then embedded into the principle component. Compared with the watermarking algorithm based on DWT, experimental results indicate that the new algorithm shows a strong robustness: it not only greatly improves the ability against geometric attacks such as anti-cropping, rotation and others, but also has good resistance to noise, change of image gray value and other attacks.

Keywords: digital watermarking; discrete wavelet transform (DWT); principal component analysis(PCA); robustness

数字水印[1-5]技术是近几年信息安全领域出现的一种新技术,它将不可察觉的信号嵌入到多媒体内容中,在多媒体内容发布传播后,从中提取出这些信息用于版权保护。如何解决算法的嵌入容量、不可见性和鲁棒性之间的矛盾一直是该项研究的热点和难点。Chu[6]提出一种离散余弦变换和抽样的半盲水印算法,将水印信息嵌入到调整后的离散余弦变换(discrete cosine transform,DCT)系数中,但算法的鲁棒性表现不好。Wang[7]提出的基于离散小波变换(discrete wavelet transform,DWT)变换和奇异值分解(singular value decomposition,SVD)算法的水印算法,能有效抵抗几何攻击,但抵抗其他攻击的鲁棒性不强。Hana 等[8]提出的算法将水印嵌入到经过 DWT 变换后的低频或高频中,鲁棒性虽然有所提高,但抗几何攻击能力仍然不足。主成分分析(principal component analysis,PCA)[9]作为模式识别领域特征降维的一种经典方法,能够采用较少数量的特征对样本进行描述,以达到降低特征空间的维

收稿日期:2014-09-12

基金项目:国家自然科学基金项目(51274232,61305008);中央高校基本科研业务费专项(14CX06008A);山东省自然科学基金项目(ZR2011FQ018)

作者简介:郑秋梅(1964-),女,教授,硕士,研究方向为数字水印、图像检索。E-mail: zhengqm@upc.edu.cn。

数,经过 PCA 提取的特征向量都是有意义且互不相关的,而且这些特征向量代表着图像最大部分的能量,既含有图像高频部分,又含有图像低频部分,将水印嵌入到这些特征向量中,水印将表现出良好的鲁棒性。笔者结合 DWT 和主成分分析,提出一种新的数字水印算法。

1 主成分分析的基本原理

主成分分析[9]是一种多元统计分析方法,它利用某些特定的原则或者方法将某一组相关变量转换成另一组不相关的变量,这些不相关变量具有按方差逐渐递减排列的特征。

设有 n 个样本 $X_1,\cdots,X_p$,p 维向量 $\boldsymbol{x}=(x_1,\cdots,x_p)^{\mathrm{T}}$,$i=1,2,\cdots,n$,$n>p$,构造样本矩阵如下:

$$\boldsymbol{X}=\begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1n} \\ X_{21} & X_{22} & \cdots & X_{2n} \\ \vdots & & & \\ X_{p1} & X_{p2} & \cdots & X_{pn} \end{bmatrix}. \tag{1}$$

主成分的基本计算过程如下:

(1)将原始数据进行基本的标准化。对样本矩阵 $\boldsymbol{X}$ 进行如下标准化变换:

$$Z_{ij}=\frac{x_{ij}-\overline{x_j}}{s_j},i=1,2,\cdots,n,j=1,2,\cdots,p. \tag{2}$$

其中

$$\overline{x_j}=\frac{\sum_{i=1}^{n}x_{ij}}{n},\ s_j^2=\frac{\sum_{i=1}^{n}(x_{ij}-\overline{x_j})}{n-1}.$$

式中,$\overline{x_j}$为均值;s_j 为 $\boldsymbol{X}$ 的分量的方差。

(2)求标准化矩阵 $\boldsymbol{Z}$ 的相关系数矩阵 $\boldsymbol{R}$。

$$\boldsymbol{R}=[r_{ij}]\boldsymbol{x}p=\begin{bmatrix} 1 & r_{12} & \cdots & r_{1p} \\ r_{21} & 1 & \cdots & r_{2p} \\ \vdots & & & \\ r_{p1} & r_{p2} & \cdots & 1 \end{bmatrix}. \tag{3}$$

其中

$$r_{ij}=\frac{\sum Z_{ij}Z_{ij}}{n-1},i,j=1,2,\cdots,p.$$

(3)求样本相关矩阵 $\boldsymbol{R}$ 的特征方程。根据下式求得 p 个特征值:

$$|\boldsymbol{R}-\lambda\boldsymbol{I}_p|=0. \tag{4}$$

并按照由大到小的顺序排列,即 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_p\geqslant 0$。根据特征值 λ_i 求出特征向量 $\boldsymbol{e}_i(i=1,2,\cdots,p)$,再由特征向量 $\boldsymbol{e}_i$ 组成特征系数矩阵 $\boldsymbol{U}=(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_p)^{\mathrm{T}}$。

(4)确定主成分数。关于主成分分析,主成分个数的确定是关键,选择不当有可能丢失一些重要信息。

将主成分[9]在整个数据分析中所占的比重定义为贡献率(R_c)。m 个主成分求和对 $\boldsymbol{X}$ 各个分量方差总和的贡献率称为累计贡献率(R_{ac})。

令 λ_i 代表第 i 个特征值,可以定义第 i 个主元素的贡献率 $R_c(r)$ 为

$$R_c(r)=\frac{\lambda_i}{\sum_{i=1}^{n}\lambda_i}. \tag{5}$$

其中 λ_i 为特征值,$i=1,2,\cdots,p$。

然后可以推出前 m 个主成分的累计贡献率 $R_{ac}(m)$:

$$R_{ac}(m)=\frac{\sum_{i=1}^{m}\lambda_i}{\sum_{i=1}^{n}\lambda_i}. \tag{6}$$

在现实应用中,为了让提取信息的总利用率达到比较好的状态,一般按照 $R_{ac}\geqslant 85\%$ 确定 m 值。

(5)变换真正的主成分。按下式计算主成分:

$$F_j=\boldsymbol{U}_j^{\mathrm{T}}\boldsymbol{Z},j=1,2,\cdots,m. \tag{7}$$

本文中提出用 PCA 对图像进行主成分分析,提取出的系数是最能代表图像特征的主成分,这些主成分既包含图像的高频部分,也包含图像的低频部分,一般的频域变换例如 DCT、DWT 等都是将图像的低频域与高频域严格分离,而针对不同的攻击,将水印嵌入到某个单独的频域中,算法将会表现出不同的鲁棒性,如 DWT 变换的几何攻击鲁棒性较差。由于主成分具有高频与低频不分离的特征,将水印嵌入到 PCA 提取的主成分中能有效避免一般频域变换算法出现的问题。本文中在充分发挥 DWT 变换优势并结合 PCA 方法的基础上,选择合适的水印嵌入算法和嵌入系数以及水印嵌入强度,可以有效提高算法的鲁棒性。

2 基于 PCA 和 DWT 的数字水印算法

2.1 水印的预处理——置乱

置乱变换是数字图像加密中广泛应用的一种方法。“置乱”顾名思义就是打乱信息的次序,使其变得难以辨认。图像置乱技术[10]利用数字图像具有数字矩阵的特点,搅乱图像中像素的位置或颜色,使之变成一幅杂乱无章的图像,以达到保密的效果;文献[10]中使用 Arnold Cat 变换算法对图像进行置

乱,该算法置乱效果好,运算也简单。本文中水印置乱方法采用文献[10]的置乱方法将水印噪声化,使得图像的能量尽可能地均匀分布,加强了算法抗裁剪方面的能力,有效提高隐藏信息的安全性和鲁棒性,并可以利用其周期性进行反变换,对图像置乱进行恢复。图 1 分别是原始水印图像和加密后水印图像,选取的密钥 $key=0.2345$。

(a) 原始水印　　(b) 加密后水印

图 1　原始水印图像和加密后水印图像

Fig. 1　Original watermark image and encrypted watermark image

2.2　基于 PCA 和 DWT 的算法嵌入过程

设原始载体图像为 $\boldsymbol{I}$,水印图像为 $\boldsymbol{W}$,加密后的水印图像为 $\boldsymbol{W}'$。具体嵌入过程如下:

(1)首先对载体图像进行 8×8 分块处理,分成一系列的子块 $\boldsymbol{I}_n(n=1,2,\cdots,4\,096)$。对每一个子块 $\boldsymbol{I}_n$ 做一级 DWT 变换,得到一个新的系数矩阵 $\boldsymbol{I}_n^{DWT}$,包括低频子带 $\boldsymbol{I}_n^{LL}(i,j)$和相应的水平、垂直、对角线方向的细节子带 $\boldsymbol{I}_n^{LH}(i,j)$、$\boldsymbol{I}_n^{HL}(i,j)$、$\boldsymbol{I}_n^{HH}(i,j)(i,j=1,2,\cdots,4)$。

(2)选取低频子带 $\boldsymbol{I}_n^{LL}(i,j)$,对 $\boldsymbol{I}_n^{LL}(i,j)$进行标准化,生成矩阵 $\boldsymbol{Z}(i,j)$。

(3)求出标准化阵 $\boldsymbol{Z}(i,j)$的相关系数矩阵 $\boldsymbol{R}(i,j)$。

(4)根据样本相关矩阵 $\boldsymbol{R}$ 的特征方程[9],求出 p 个特征根,并按照由大到小的顺序排列,即 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_p\geqslant0$。求出特定特征值 λ_i 后,就可以根据特征值求得需要的特征向量 $\boldsymbol{e}_i(i=1,2,\cdots,p)$,然后利用特征向量 $\boldsymbol{e}$ 可以组成特征系数矩阵为 $\boldsymbol{U}=(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_p)^{\mathrm{T}}$。

(5)变换真正的主成分。计算公式为

$$\boldsymbol{y}_j=\boldsymbol{U}_j^{\mathrm{T}}\boldsymbol{Z},j=1,2,\cdots,m. \tag{8}$$

(6)水印嵌入。

$$Y'=y+aw. \tag{9}$$

式中,m 为提取的主成分个数;a 为水印嵌入强度;y 为嵌入前的主成分系数,Y'为含水印的主成分系数。

将嵌入后的主成分系数 Y'按照嵌入过程逆变换回去生成含水印的载体图像 $\boldsymbol{I}^W$。

步骤(1)、(2) 将载体图像分块进行一级 DWT 变换选取低频子带 $\boldsymbol{I}_n^{LL}(i,j)$,因为低频子带代表着图像的大部分信息能量,将水印固定嵌入到这部分区域中能有效地抵抗攻击,为后面进行 PCA 主成分分析选择了合适的区域。步骤(3) ~ (5) 是将每一块图像的低频区域进行了主成分分析,求得每一块的主成分,这些主成分既代表高频部分又代表低频部分,将水印嵌入到这些主成分中能有效提高鲁棒性。步骤(6)是选择合适的水印嵌入强度并根据公式(9)将水印嵌入到主成分中。

选取不同的水印控制系数,会影响水印的鲁棒性和不可见性,因为嵌入法则采用的是系数加法原则,所以当 a 越大,鲁棒性越好,但不可见性变差,a 可以通过实验经验来选取,对于不同的图像可以有所变化,根据经验值本文中 a 选取 0.03。

2.3　基于 PCA 和 DWT 的算法提取过程

在水印提取过程中,根据置乱后的密钥 key[10] 和嵌入的水印强度值 a 完成整个水印提取。详细步骤如下:

(1)将原始载体图像 $\boldsymbol{I}$ 按照嵌入过程的前五步得出原始主成分 $y_i(i=1,2,\cdots,m)$。

(2)将含水印图像 $\boldsymbol{I}^W$ 也按照嵌入过程的前五步得出新的主成分 $Y'_i(i=1,2,\cdots,m)$。

(3)提取水印。

$$w=(Y'-y)/a. \tag{10}$$

式中,w 为提取的水印。

载体图像经 DWT[11] 变换后会分解成低频、水平、垂直、对角线方向的 4 个子带,低频子带代表着图像最大的信息能量,将水印嵌入低频子带中比嵌入到其他 3 个子带中鲁棒性表现更强,在低频子带的基础上再进行 PCA 主成分分析提取图像的主成分,这些主成分最能代表图像特征,既包含图像的高频部分,也包含图像的低频部分,将水印嵌入到这些主成分中,能很好地解决只嵌入低频部分引起的图像失真过大问题,而且鲁棒性表现仍然很强。

3　实验及分析

3.1　数字水印评价标准

3.1.1　峰值信噪比

峰值信噪比[12](peak signal to noise ratio, PSNR)可用来定量描述图像的失真程度。峰值信噪比值越大,表示两幅图像越相似,即图像的保真度越好。一般而言,当峰值信噪比大于 33 dB 时,人眼视觉就无法区分两幅图像的差别,认为两幅图像是一样的。峰值信噪比 R_{PSN}的计算公式为

$$R_{\mathrm{PSN}}=10\lg\left[\frac{MN\max(\boldsymbol{I})^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(\boldsymbol{I}-\boldsymbol{I}')^2}\right]. \tag{11}$$

式中,$\boldsymbol{I}$ 为原始载体图像,$\boldsymbol{I}'$ 为含水印图像;M、N 表示图像的大小。

3.1.2 归一化相关系数

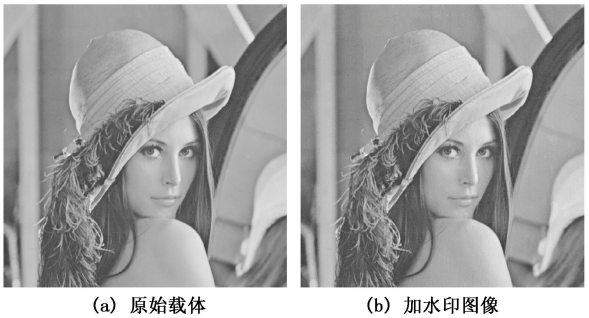
归一化相关系数[12] 用来衡量原始水印与提取水印之间的相似度。对于鲁棒性水印,归一化相关系数值越大越好;而对于脆弱水印,归一化相关系数值越小越好。其计算公式为

$$NC = \frac{\sum_{i=1}^{L} w(i) * w'(i)}{\sqrt{\sum_{i=1}^{L} w^2(i)} \sqrt{\sum_{i=1}^{L} w'^2(i)}}. \quad (12)$$

式中,NC 为归一化系数;$w(i)$ 为原始水印信息;$w'(i)$ 为提取出的水印信息;L 为水印信息的长度。

3.2 实验结果及分析

通过峰值信噪比来评价算法的图像保真度性能,图 2 分别是原始载体图像和加水印后图像,实验测得原始载体图像和含水印图像间的峰值信噪比为 44.8627。当峰值信噪比大于 33 时,图像之间具有良好的相似性[1-3,6-8,12],因此本文算法很好地实现了水印的不可见性。



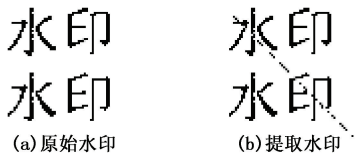
(a) 原始载体 (b) 加水印图像

图 2 原始载体图像和加水印后图像

Fig. 2 Original image and watermark image

分别对本文算法进行无攻击、裁剪、旋转、增加积性噪声、增加高斯噪声、图像增亮、图像变暗、直方图均衡化、增加和降低对比度等攻击(图 3 ~ 8),实验所得归一化系数值如表 1 所示。

图 3 显示的是原始水印图像和提取的水印图像,图像在进行 PCA 主成分分析时,提取的主成分是一个对角矩阵,将水印嵌入到这些主成分中虽然能有效地抵抗攻击,但是在变换和逆变换过程中自身会失去一些信息。图 4 ~ 8 分别是本文算法和文献[8]算法在受到裁剪、旋转 45°、高斯噪声、图像增亮和降低对比度攻击后提取的水印图像。无论是从表 1 实验数据还是从提取的水印效果图像上看,本文算法除了在无攻击情况下的性能比文献[8]的稍差外,在抗裁剪、旋转、图像灰度值变化攻击性能都好于文献[8],并且旋转和缩放的归一化系数值明显高于文献[8]。由于本文中充分利用 DWT 变换和 PCA 算法将水印信息嵌入到最佳的系数中,因此较好地保证了水印结构的完整性。



(a)原始水印 (b)提取水印

图 3 原始水印图像和提取的水印图像

Fig. 3 Original watermark and watermark image extracted

(a)裁剪 (b)本文算法 (c)文献[8]

图 4 裁剪攻击

Fig. 4 Cropping attack

(a)旋转45° (b)本文算法 (c)文献[8]

图 5 旋转攻击

Fig. 5 Rotation attack

(a)高斯噪声 (b)本文算法 (c)文献[8]

图 6 高斯噪声攻击

Fig. 6 Gaussian noise attack

(a) 图像增亮　(b) 本文算法　(c) 文献[8]

图 7　图像增亮攻击

Fig. 7　Image enhancement attack

(a) 降低对比度　(b) 本文算法　(c) 文献[8]

图 8　降低对比度攻击

Fig. 8　Reduced contrast attack

表 1　受各种攻击后提取水印的归一化系数值

Table 1　Normalized cross correlation of extracting watermark after attacks

攻击类型	攻击参数	本文算法	文献[8]
无攻击		0.9951	1.0000
裁剪	左上角 1/5	0.9908	0.9687
旋转	45°	0.9927	0.6676
积性噪声	0.01	0.9936	0.8797
高斯噪声	0.01	0.9941	0.7990
图像增亮	[0.4,1]	0.9948	0.7597
图像变暗	[0,0.95]	0.9951	0.9978
直方图均衡化		0.9937	0.9831
增加对比度	[0.2,0.6]	0.9933	0.8822
降低对比度	[0.2,0.8]	0.9950	0.7606

4　结束语

本文中提出了一种 DWT 结合 PCA 的数字水印算法,将置乱后的水印利用加法原则嵌入到算法提取的主成分中。实验结果证明,与传统 DWT 水印算法相比,该算法不仅明显提高了抗剪裁、旋转等抗几何攻击能力,对加噪、图像灰度值变化等攻击也表现出了很强的鲁棒性。算法可在数字内容认证、版权保护等方面进行推广。本文算法也存在一些不足,如算法未攻击时提取的水印稍差、算法提取主成分时算法效率不高等问题,如何解决这些问题是下一步工作的重点。

参考文献:

[1] 郑秋梅,杨发科,蒋晓红. 一种基于关系的小波域水印算法[J]. 中国石油大学学报(自然科学版),2009,33(2):164-168.
ZHENG Qiumei, YANG Fake, JIANG Xiaohong. A digital watermarking algorithm based on relationship in wavelet transform domain [J]. Journal of China University of Petroleum(Edition of Natural Science), 2009,33(2):164-168.

[2] 郑秋梅,顾国民,王玉菲,等. 一种新的抗几何攻击的数字算法[J]. 中国石油大学学报(自然科学版),2012,36(1):188-192.
ZHENG Qiumei, GU Guomin, WANG Yufei, et al. A novel digital watermarking algorithm against geometric attacks [J]. Journal of China University of Petroleum(Edition of Natural Science), 2012,36(1):188-192.

[3] LANGELAAR G C, SETYAWAN I, LAGENDIJK R L. A state-of-the-art overview [J]. IEEE Signal Processing Magazine, 2000,17(5):20-46.

[4] BERGMAN C, DAVIDSON J. Unitary embedding for data hiding with the SVD [C/OL]//Security, Steganography, and Watermarking of Multimedia Contents VII, January 17-20, 2005 [2014-01-11]. http://www.researchgat. net/publication/221011223_Unitary_embedding_for_data_hiding_with_the_SVD.

[5] ASLANTAS V. An optimal robust digital image watermarking based on SVD using differential evolution algorithm [J]. Optics Communications, 2009,282(5):769-777.

[6] CHU W C. DCT-based image watermarking using subsampling [J]. IEEE Transactions on Multimedia, 2003,5(1):34-38.

[7] WANG Y. Digital watermarking algorithm based on SVD and DWT [J]. Computer Simulation, 2011,28(5):295-298.

[8] HANA O, HELA M, KAMEL H. A robust multiple watermarking scheme based on the DWT [C/OL]//2013 10th International Multi-Conference on Systems, Signals & Devices (SSD), March 18-21, 2013 [2014-02-12]. http://ieeexplore. ieee. org/stamp/stamp. jsp? tp = &arnumber=6564024.

[9] KUNCHEVA L I, FAITHFULL W J. PCA feature extraction for change detection in multidimensional unlabeled data [J]. Neural Networks and Learning Systems, IEEE Transactions on, 2014,25(1):69-80.

[10] WANG Jizhi, WANG Yinglong, WANG Meiqin. Perio-

dicity and application for a kind of n-dimensional Arnold-type Transformation [C/OL]//Intelligence and Security Informatics. May 23-24, 2007 [2014-03-11]. http://ieeexplore. ieee. org/stamp/stamp. jsp? tp = &arnumber=4258735.

[11] REYES R, CRUZ C, NAKANO-MIYATAKE M, et al. Digital video watermarking in DWT domain using chaotic mixtures [J]. Latin America Transactions, IEEE (Revista IEEE America Latina), 2010,8(3):304-310.

[12] 郑秋梅,金萧,顾国民,等. 一种基于 Data Matrix 的数字水印算法[J]. 中国石油大学学报(自然科学版),2015,39(1):188-193.
ZHENG Qiumei, JIN Xiao, GU Guomin, et al. A digital watermarking algorithm based on Data Matrix [J]. Journal of China University of Petroleum(Edition of Natural Science), 2015,39(1):188-193.

(编辑 修荣荣)