

# 傅里叶相位图水印隐藏的实现与应用

王海燕, 刘结焱, 陈圆美

(安徽大学 计算智能与信号处理教育部重点实验室, 安徽 合肥 230039)

**摘要:**采用待隐藏图像的相位图作为数字水印嵌入宿主图像,实现了信息隐藏,与隐藏图像同时具有振幅信息和相位信息的情况比较,需要隐藏的信息量显著降低。相应的水印提取数据仅是图像的相位信息,并将提取出的傅里叶相位图像与一幅新图像的傅里叶振幅图像结合,原始隐藏图像被恢复,验证了图像的相位的主导性,且运用这种特性可有效地实现信息的隐藏与恢复。利用图像所具有的迷惑性产生的信息隐藏更能起到掩护的作用。

**关键词:**傅里叶相位图; 数字水印; 信息隐藏

**中图分类号:**TP309

**文献标识码:**A

**文章编号:**1673-629X(2011)04-0175-04

## Implementation and Applications of Fourier Phase Image Digital Watermarking Hiding

WANG Hai-yan, LIU Jie-yan, CHEN Yuan-mei

(Ministry of Education Key Lab. of Intelligent Computing and Signal Processing,  
Anhui University, Hefei 230039, China)

**Abstract:** Used the Fourier phase of to be hidden image as a digital watermarking embedded in a host image, implemented information hiding. In comparison with hidden image consists of amplitude and phase information, the need to hide the amount of information is greatly reduced. The corresponding extracted data only is phase information, this phase and another unrelated Fourier amplitude image are used to reconstruct the original hidden image, which verifies the phase dominance, and using this property can effectively implement information hiding and reconstruction. The way of using delusion of digital image for data hiding can play better protective role.

**Key words:** Fourier phase image; digital watermarking; information hiding

## 0 引言

由于现代社会互联网的发达,如今越来越多的人依赖多媒体进行信息交流和传递重要信息。特别是文本、图像的随意篡改问题日益严重。网络的不断发展也使人们更多的注意力投放到信息隐藏上<sup>[1]</sup>。20世纪90年代中后期信息隐藏技术逐渐受到人们的关注与重视,信息隐藏的安全性也随着近年来信息隐藏技术已经成为一个研究热点。

数字图像水印技术是信息隐藏和信息安全技术领域的一个重要的分支,可以在很多领域得到应用,它的出现为知识产权的保护提供了有力的保障。数字水印技术已经成为数字产权保护的主要技术<sup>[2]</sup>。数字水印与密码技术不同的是:密码技术对于数据传输十分有用,却无法在编码后对原始数据提供检查的方法;数字水印不同于密码技术,它仍然具有数据的原始形式,而

且不会妨碍用户收听、观看、检验或者操作数据<sup>[3]</sup>。

## 1 信息隐藏

### 1.1 信息隐藏基本概念

信息隐藏技术(Information Hiding),是利用人类感官系统的不敏感,载体信息中具有随机特性的冗余部分,将隐藏信息以某种方式嵌入到载体信息之中,使其不被他人发现或不易被察觉。

一般载体可以是图像文件、文本文件、数字音频格式的音频、视频或网络协议等数字信号。它有两项重要的应用。一是可以实现机要信息的安全隐蔽通信。即利用信息隐藏技术,将秘密信息携带在各种正常的多媒体载体中,将秘密信息正被传递的事实进行掩盖,以“瞒天过海”的手段达到信息安全隐蔽传递的目的。应用二是可以实现多媒体作品的版权管理。即将作品的版权信息等嵌入到数字产品中,达到版权认证、盗版追踪、篡改发现等目的<sup>[4-6]</sup>。

### 1.2 信息隐藏的特征

根据不同媒体进行信息隐藏各自具有不同的特

收稿日期:2010-09-03;修回日期:2010-12-13

基金项目:国家自然科学基金资助项目(60603083,60872106)

作者简介:王海燕(1987-),女,安徽人,硕士研究生,研究方向为计算机视觉、相位恢复。

点,通常将信息隐藏的基本特征概括为以下几个方面:

(1) 安全性(Security):安全性指的是攻击者在不知道隐藏算法和密钥时,不能够阅读和修改被隐藏的秘密信息。

(2) 感知质量(Perceptibility):是指秘密信息的嵌入到载体中不应导致明显的感知失真。当秘密信息按照一定方式嵌入载体后,载体不可被觉察出明显的人为痕迹。信息隐藏对人的感觉系统是透明的,如人的视觉感知或听觉感知。如向一幅载体图片文件中添加水印秘密信息,人的肉眼无法察知宿主图像与伪装图像之间的差别。

(3) 稳定性(Stability):稳定性指的是隐藏的秘密信息能“永久”的存在,并在一定的条件下可以提取。

(4) 鲁棒性(Robustness):鲁棒性指的是嵌入载体中的秘密信息能够承受一定的施加于载体的变换操作,仍能恢复被隐藏的信息。鲁棒性要求数据嵌入算法能保证嵌入数据在经受一定变换后的可检测性或可恢复性。

(5) 隐藏容量(Capacity):是指载体可以承载秘密信息的最大值。嵌入的秘密信息量必须能够满足表达一定的意义的,如能够表示某一图片信息的版权等,否则嵌入的信息量较少,这样的嵌入是没有意义的。通常隐藏容量与要实现隐藏而达到的不可见性、鲁棒性、载体分布等因素都有关。其中与鲁棒性的关系最为明显,嵌入的秘密信息量以一定方式增加时,系统的鲁棒性会相对减弱。

## 2 数字水印

### 2.1 数字水印的分类

数字水印技术是通过一定的算法将一些标志性信息直接嵌入到多媒体内容当中,但不影响原内容的价值和使用,并且不能被人的感知系统觉察或注意到,只有通过专用的检测器或阅读器才能提取的一种技术。一个数字水印系统一般包括 3 个基本方面:水印的生成、水印的嵌入和水印的提取或检测<sup>[7,8]</sup>。

基于图像的水印隐藏技术大体可以分为两种:基于时空域的数字水印技术和基于频率域的数字水印技术。

(1) 基于时空域的隐藏技术相对简单,时空域数字水印技术中,嵌入图像的水印信息不经过任何变换,直接嵌入到图像像素上<sup>[9]</sup>。常采用最不重要位(LSB)嵌入法,即是利用人对图像的视觉冗余,把水印图像嵌入到载体图像像素点的最不重要位上。可以在载体图像像素点比特位的最低一位或者最低几位上添加水印,这种时域上的隐藏方法简单有效,信息隐藏量大。

(2) 基于变换域的隐藏技术首先把载体变换到变

换域,变换域的数字水印技术中将图像和水印变换到不同的域(常用的有小波变换域、频率变换域、离散傅里叶变换域、离散弦变换域等其中任何一种)上实现水印的嵌入<sup>[9]</sup>。将信息隐藏在变换域的系数中,通常一种变换对应着一种水印嵌入的方法。这种频域上的隐藏方法稳健性良好,能够对抗多种攻击。

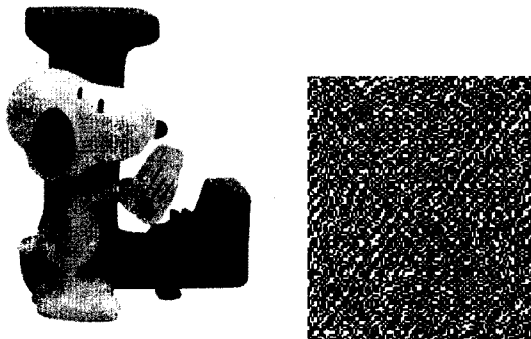
### 2.2 LSB 空域法原理

LSB(最低有效位或最不重要位)是空域法中基础而最为重要的方法之一,也可以理解为替换法。LSB 算法有其隐蔽性好、信息隐藏量大且易于实现等优点<sup>[10]</sup>。人的生理特点决定了人眼只能识别大概 40 级灰度,我们试图用机密信息比特替换掉载体中不重要的部分,达到对秘密信息编码的目的。一幅灰度图像载体,它由许多像素点构成,一幅 256 级灰度图中每一个像素是由 8 位二进制构成。例如 11111111(255), 00000000(0),其中每一位在这个像素所起到的作用是不一样的,最高位就代表 10000000(128),接着依次每一位的 1 分别代表 64、32、16、8、4、2、1,可见当到达最后一位时,最低位 1 只代表 1,这时它所起到的作用是很小的。根据人眼对最低位的最不敏感性,若对 256 级灰度的每一个像素值的最低位修改,其误差率  $\leq 1/255$ ,这给水印带来了最直接的提示,可以通过改变一幅图像的最低位来嵌入数据。因为即使载体图像的所有最低位都改变了,图像本身也基本不会发生任何变化,即满足了水印的透明性。因为对图像的每一个像素值都可以修改进而嵌入水印,可以看出这种方法隐藏信息量非常大。

## 3 实验

按照上述原理,可以由以下几个步骤来完成水印的嵌入提取及利用提取的信息实现图像的恢复。这里采用待隐藏图像的相位图作为数字水印。

(1) 获取相位图。首先确定待隐藏的图像为图片 L.jpg,图像经过傅里叶变换,由此获得它的相位图像相位 L。如图 1 所示。



(a) 图片 L

(b) 获取的相位

图 1 由待隐藏图像获取相位图

(2) 相位图的隐藏和提取。实验采用标准灰度图像“lena.jpg”作为宿主图像,参见图 2(a)。水印图像采用图 1(b)变换后的图像,由于相位图的像素值已不是完全整型的数值,这里采用线性变换,算出像素值的最大值 MAX 和最小值 MIN,由这两个值可以将图像中每一点的像素值等比例的改变为 0 到 255 中的值,其中最小值 MIN 对应变换为 0 值,最大值 MAX 对应变换为 255 值。这时可将 256 级灰度图中每一个像素转化为 8 位二进制构成,参见图 2(b)。可见真正嵌入的水印图像实则为二值图像,这样就可利用水印原理把机密信息比特替换掉宿主图像中不重要的部分,达到对秘密信息编码的目的。添加水印后的伪装图像,参见图 2(c)。水印算法仿真实验环境为 MATLAB 7.5.0。

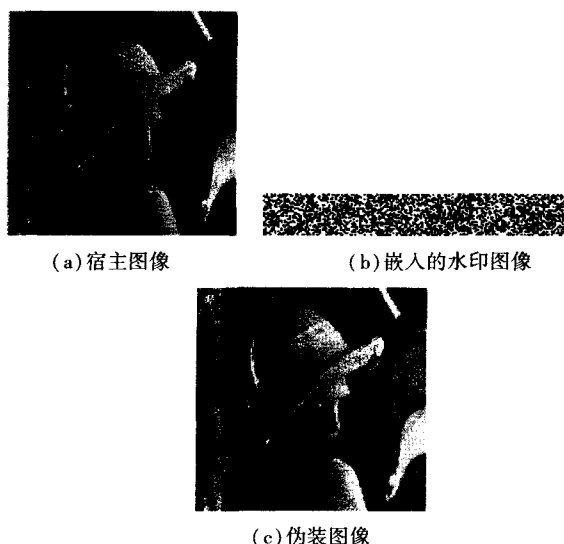


图2 水印的嵌入过程

水印的提取过程是编码隐藏的逆过程,这里不多叙述。提取的水印图像参见图 3(a)。再将提取出的二值水印图像逆转化为 256 级灰度图像,利用之前算出的最大值 MAX 和最小值 MIN,由这两个值可以将 256 级灰度图像中每一点的像素值等比例的变换到最小值 MIN 到最大值 MAX 区间内的值,其中 0 值对应变换为最小值 MIN,255 值对应变换为最大值 MAX,得到恢复的相位,参见图 3(b)。

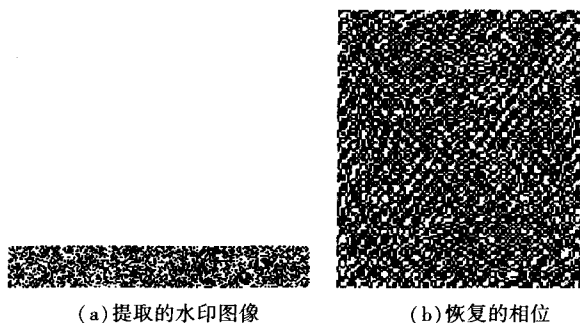


图3 提取的水印图与恢复

(3) 由相位图恢复原始图像。一幅图像有振幅信息和相位信息构成,文献[11,12]中论述了可以由图像的相位信息来恢复原图像,相位具有主导作用。这一步骤我们做了两种尝试:第一利用恢复的图像 L 的相位,图像 J.jpg 的振幅,恢复出 L 的图像。这里 J 是一幅与 L 相似度很高的图像,图像 J.jpg 以及它的傅里叶振幅图参见图 4(a)与图 4(b)。运行程序,原始图像 L 的图像被成功的恢复出来。下面给出了原始图像与恢复图像的对比图,参见图 4(c)与图 4(d)。

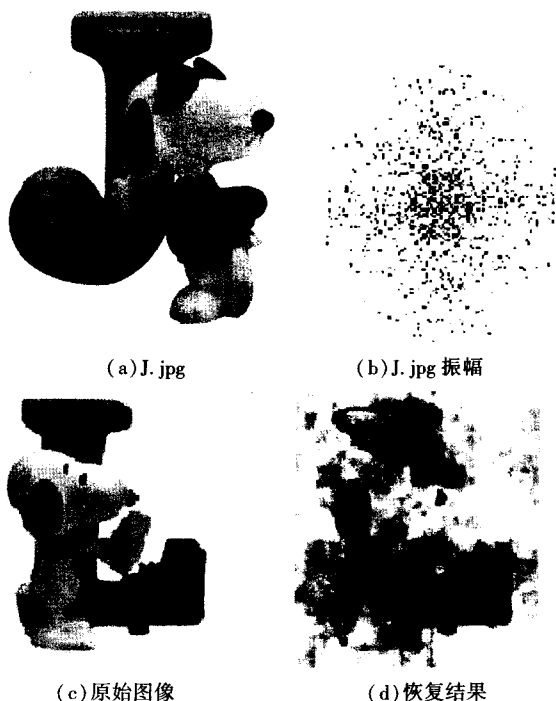


图4 由相位信息与振幅信息恢复原始图

第二利用恢复的图像 L 的相位,图像 lena.jpg 的振幅,恢复出 L 的图像。这里 lena.jpg 是一幅与 L 相似度较低的图像,图像 lena.jpg 以及它的傅里叶振幅图参见图 5(a)与图 5(b)。运行程序,原始图像 L 的图像也可顺利的恢复出来。下面给出了原始图像与恢复图像的对比图,参见图 5(c)与图 5(d)。

实验表明,当使用的辅助图像与待恢复图像有较高相似度时,待恢复图像的相位信息借助于辅助图像的振幅信息,可以有效地恢复出原始图像的画面。

## 4 结束语

采用待隐藏图像的相位图作为数字水印嵌入宿主图像,与隐藏图像同时具有振幅和相位信息的情况比较,需要隐藏的信息量显著降低。目前有多种水印隐藏技术可以利用,文中选用的是 LSB 法。利用空域 LSB 法实现信息隐藏有其必要的优点,如它的简易性、不可见性和一定的健壮性,最主要是这种方法隐藏信息量非常的大。并且通过利用其最基础的原理,加上

图形图像知识,实现了灰度图像的隐藏,隐藏的信息量也明显降低。

文中最重要的是实现了提取出的傅里叶相位图像与一幅新图像的傅里叶振幅图像结合,原始隐藏图像被恢复,验证了图像相位的主导性,且运用这种特性可有效地实现信息的隐藏与恢复。将数字水印技术与图像傅里叶的相位特性结合,在信息隐藏与恢复方面有明显的应用前景。

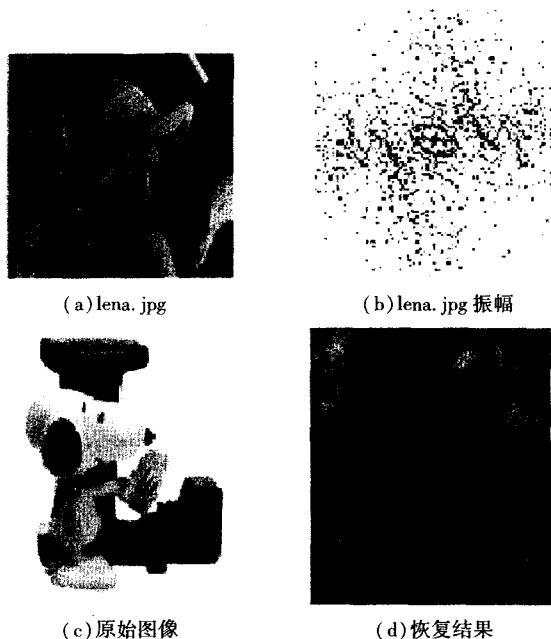


图 5 由相位信息与振幅信息恢复原始图

#### 参考文献:

- [1] GE Xiu-hui, TIAN Hao. Research on information hiding theoretic model[J]. Electronic Measurement and Instruments, 2007(2): 227-232.
  - [2] JIAN Zhao, Koch E. A Generic Digital Watermarking Model[J]. Computer & Graphics, 1998, 22(4): 397-403.
  - [3] 刘晓柯, 苏显渝. 基于图像部分加入的数字全息水印技术[J]. 光子学报, 2008, 37(4): 740-744.
  - [4] 钮心忻. 信息隐藏与数字水印[M]. 北京: 北京邮电大学出版社, 2004.
  - [5] 韩东初, 刘緬方. 基于文本的信息隐藏技术研究[J]. 计算机安全, 2008(8): 60-63.
  - [6] 李丽娟, 熊淑华. 基于文本的信息隐藏技术研究[J]. 现代电子技术, 2006, 29(5): 67-69.
  - [7] 孙依薇, 杨武剑. 信息隐藏在数字签名中的研究[J]. 电子科技大学学报, 2009, 38(11): 49-52.
  - [8] 于帅珍, 冯丽平. 数字水印的关键技术[J]. 计算机技术与发展, 2010, 20(2): 148-151.
  - [9] 张勇, 赵东宁, 李德毅. 数字水印技术及发展[J]. 解放军理工大学学报(自然科学版), 2003, 4(3): 1-5.
  - [10] 袁占亭, 张秋余, 刘洪国, 等. 一种改进的 LSB 数字图像隐藏算法[J]. 计算机应用研究, 2009, 26(1): 372-374.
  - [11] Hayers M H. The reconstruction of a multidimensional sequence from the phase or magnitude of the FFT[J]. IEEE Transactions on ASSP, 1992, (4): 140-154.
  - [12] Hsiao Wen-Hsin, Hons B E, Sci B. Aspects of Fourier imaging[D]. New Zealand: University of Canterbury Christchurch, 2008.
- 
- (上接第 174 页)
- 商代码丢失了, 加密技术也可以通过改进加密的算法, 或是用户自选择其他的编码密码。
- #### 参考文献:
- [1] Strategy Analytics[EB/OL]. 2010-09-21. <https://www.strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=4936>.
  - [2] 世界电子元器件. 无钥匙门禁系统完全解决方案[J]. 世界电子元器件, 2009(7): 1-2.
  - [3] MICROCHIP. Using the PIC16F639 MCU for Smart Wireless Application. pdf[EB/OL]. 2005. [http://www.microchip.com/stellent/idcplg?IdcService=SS\\_GET\\_PAGE&nodeId=1824&appnote=en021451](http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1824&appnote=en021451).
  - [4] 王浩远, 梁昌勇, 俞家文, 等. 基于 RFID 技术的汽车总装 MES 系统研究[J]. 计算机发展与技术, 2010, 20(9): 222-226.
  - [5] Low-Frequency Magnetic Transmitter Design[EB/OL]. 2010-09-21. <http://www1.microchip.com/downloads/en/AppNotes/00232B.pdf>.
  - [6] 刘正琼. 智能 PKE 系统设计[J]. 仪器仪表学报, 2007, 28(4): 319-322.
  - [7] MICROCHIP. Passive Keyless Entry (PKE) Reference Design User's Manual[EB/OL]. 2010-09. [http://www.microchip.com/stellent/idcplg?IdcService=SS\\_GET\\_PAGE&nodeId=1406&dDocName=en024488&part=APGRD001](http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=1406&dDocName=en024488&part=APGRD001).
  - [8] 李学海. PIC 单片机原理[M]. 北京: 北京航空航天大学出版社, 2004.
  - [9] MICROCHIP. PIC16F639 Datasheet[EB/OL]. 2010-09. <http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en022266>.
  - [10] 袁刚. PKE 系统中滚码技术的软件实现[J]. 合肥工业大学学报, 2009, 32(12): 1859-1862.
  - [11] 董辉, 卢建刚. 一种基于 KEELOQ 的改进加密算法及其在单片机中的实现技术[J]. 电子技术应用, 2004(9): 14-17.
  - [12] HCS365 datasheet[EB/OL]. 2010-09-21. <http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010765>.