基于相移干涉术的光学信息隐藏系统的软件实现*

范德胜[1)] 孟祥锋[1)†] 杨修伦[1)] 王玉荣[1)] 彭翔[2)] 何文奇[2)]

1) (山东大学信息科学与工程学院光学系, 山东省激光技术与应用重点实验室, 济南 250100)

2) (深圳大学光电工程学院, 光电子器件与系统教育部/广东省重点实验室, 深圳 518060)

(2012 年 5 月 27 日收到; 2012 年 6 月 15 日收到修改稿)

结合双随机相位编码技术与相移干涉术, 提出了一种信息隐藏系统, 待隐藏信息被加密到多幅干涉图数据中后, 通过选取合适的权重因子, 它们可以被嵌入到宿主图像中; 利用特定的相移再现公式和逆菲涅耳衍射变换, 可以实现隐藏信息的提取及解密. 通过基于 Matcom 的 Visual C++ 与 Matlab 混合编程, 设计和开发了一款信息隐藏系统软件, 经过界面测试, 该软件可以实现图像读取及显示、基本几何参数输入、信息加密及嵌入、信息提取及解密、鲁棒性测试等主要功能.

关键词: 图像加密和水印, 相移干涉术, 数字图像处理

PACS: 42.40.Kw, 42.87.Bg, 07.05.Pj, 42.30.Rx

1 引 言

自 1995 年 Javidi 等提出基于光学 4f 傅里叶变换系统的双随机相位板编码图像加密技术以来 [1,2], 光学信息加密与隐藏技术已成为信息安全领域的研究热点, 吸引着越来越多的科研工作人员投身到这一全新领域的研究中.

光学信息安全系统一般采用傅里叶变换、光学全息、远场和近场衍射、分数傅里叶变换、相位恢复技术、偏振编码等光学信息处理技术, 来实现信息的加密、嵌入、隐藏或有效提取 [3−9]. 与传统的计算机或电子安全系统相比, 光学信息安全系统具有多加密维度、高并行度、能快速实现卷积和相关运算等特点, 因而探索和开发光学信息加密和隐藏技术具有很高的学术和应用价值.

Javidi 和 Nomura 结合双随机相位编码和数字全息技术, 对光学信息加密技术进行了系统的研究. 但是, 在同轴数字全息中, 再现像会受到孪生像的干扰; 在离轴数字全息中, 记录器件 (一般为电荷耦合元件, charge-coupled device, CCD) 的分辨率比传统全息干版的分辨率低很多, 因此要求物光与参考光的夹角比较小, 这无疑给离轴数字全息的应用带来限制 [10].

Yamaguchi 等将相移算法引入到数字全息中, 通过相移干涉术采用的同轴光路记录多幅干涉图, 可以完全弥补同轴数字全息和离轴数字全息的各自不足 [11]. 由于相移干涉术具有这一明显优势, 我们先后提出了一系列光学信息加密及隐藏理论, 主要结合菲涅耳域的双随机相位编码技术, 把待隐藏信息加密到多幅干涉图信息中, 然后, 通过特定的相移再现公式和逆菲涅耳衍射解密出秘密信息 [12−16]. 在我们此前提出的这些信息加密理论之上, 本文采用基于 Matcom 的 Visual C++ 与 Matlab 混合编程设计模式, 设计和开发一款信息隐藏系统应用软件, 该软件主要采用面向对象的设计模式和管理模块化的思想, 开发出的应用软件界面美观简洁, 软件可执行性强. 以下我们首先介绍基于三步相移干涉术的光学信息隐藏系统的基本原理, 然后详细阐述信息隐藏软件的具体设计流程和方案, 最

* 国家自然科学基金 (批准号: 60907005, 61171073, 61275014)、山东省自然科学基金 (批准号: ZR2011FQ011)、山东省科技计划项目 (批准号: 2011GGH20119)、山东省优秀中青年科学家科研奖励基金 (批准号: BS2011DX023)、深圳市科技研发资金 (批准号: 0014632063100426032) 和山东大学自主创新项目 (批准号: 2010TB019) 资助的课题.

† E-mail: xfmeng@sdu.edu.cn

后给出软件界面和部分性能测试结果.

2 理论分析

2.1 信息加密及嵌入

基于三步相移干涉术的信息加密及隐藏系统的原理简图如图 1 所示 [12−14], 假设两个随机相位板 ψ_1 和 ψ_2 分别放置在输入平面 $(x_{\rm o}, y_{\rm o})$ 和变换平面 $(x_{\rm t}, y_{\rm t})$ 上, 相位板 ψ_1 和 ψ_2 是 [0, 1] 之间随机分布的白噪声, 二者的复振幅分布可以分别表示为 $\exp(\mathrm{i}2\pi\psi_1)$ 和 $\exp(\mathrm{i}2\pi\psi_2)$, 当输入平面上的待加密图像 f 被波长为 λ 的平面波照射后, 记录平面 (x, y) 上的复振幅场可以表示为 [12−16]

$$\begin{aligned} U(x,y) =& \mathrm{FrT}\big\{\mathrm{FrT}\big\{f(x_{\rm o},y_{\rm o}) \\ &\times \exp[\mathrm{i}2\pi\psi_1(x_{\rm o},y_{\rm o})];\lambda,z_1\big\} \\ &\times \exp[\mathrm{i}2\pi\psi_2(x_t,y_t)];\lambda,z_2\big\}, \end{aligned} \tag{1}$$

其中 z_1 表示输入平面 $(x_{\rm o}, y_{\rm o})$ 与变换平面 (x_t, y_t) 之间的距离, z_2 表示变换平面 (x_t, y_t) 与记录平面 (x, y) 之间的距离, FrT{.}表示菲涅耳变换.

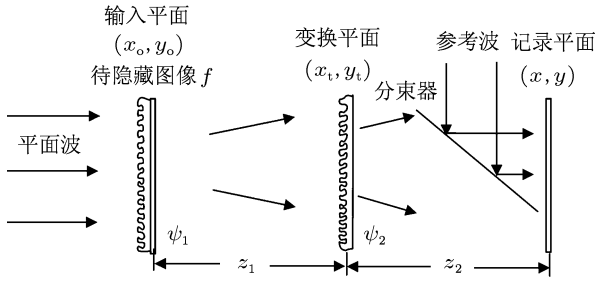

图 1 信息加密及隐藏系统的原理简图

在记录平面, 引入一振幅为 $A_{\rm r}$ 的同轴参考光与物光曝光干涉, 假设二者第 j 次曝光时, 由相移器引起的参考光的相位为 $\delta_n(0 \leqslant \delta \leqslant \pi)$, CCD 记录的光强分布为

$$\begin{aligned} I_j(x,y) =& A^2(x,y) + A_{\rm r}^2 + 2A_{\rm r}A(x,y) \\ &\times \cos[\varphi(x,y) - \delta_j], \quad j = 1\text{—}3, \end{aligned} \tag{2}$$

其中, A 和 φ 分别表示 $U(x, y)$ 的实振幅和相位分布. 我们采用三步标准相移干涉术 (三次干涉时, 参考光 δ_n 的相位分别为 0, $\pi/2$ 和 π), 可以得到三幅被相位板调制且含有隐藏信息的干涉图 I_1, I_2 和 I_3; 选同一幅宿主图像 $H(x, y)$, 对三幅干涉图依次施加三次水印嵌入后, 得到的含水印图像可以表示为

$$I'_j(x,y) = H(x,y) + wI_j(x,y), \quad j = 1\text{—}3, \tag{3}$$

其中 w 表示权重因子, 用于调节水印信息的不可感知性.

2.2 水印提取及解密

授权方得到所有密钥 (随机相位板及几何参数) 后, 利用含水印图像可以通过下面的步骤提取水印并解密出原始图像:

1) 通过标准三步相移公式, 可以得到经权重因子调制后的记录平面上的复振幅场信息

$$wU = \frac{I'_1 - I'_3 + \mathrm{i}(2I'_2 - I'_1 - I'_3)}{4A_{\rm r}}, \tag{4}$$

当系统未受到任何攻击时, 由于最后的解密图像都需要实振幅归一化, 权重因子 w 的选取并不影响隐藏信息的提取及解密. 需要指出的是, 当系统受到各种攻击时, 一般权重因子 w 越大, 嵌入的信息量会增加, 系统的鲁棒性就会越好, 但随着权重因子的增大, 含水印图像的不可感知性 (或不可见性、隐蔽性) 会变差. 因此, 信息的嵌入量与不可感知性之间存在着矛盾, 随着嵌入信息量的增加, 水印载体的质量必然下降. 所以, 选取的权重因子 w 既不能过大也不能过小, 需要综合考虑不可感知性与鲁棒性两方面的因素, 来折中选取比较合适的权重因子 w.

2) 通过两次逆菲涅耳变换, 恢复出物体平面上的经权重因子调制的复振幅场

$$\begin{aligned} wU_{\rm o}(x_{\rm o},y_{\rm o}) =& \mathrm{IFrT}\big\{\big\{\mathrm{IFrT}[wU(x,y);\lambda,z_2] \\ &\times \exp[-\mathrm{i}2\pi\psi_2(x_t,y_t)]\big\};\lambda,z_1\big\} \\ &\times \exp[-\mathrm{i}2\pi\psi_1(x_{\rm o},y_{\rm o})], \end{aligned} \tag{5}$$

其中, IFrT 表示逆菲涅耳衍射.

3) 提取复振幅场 $wU_{\rm o}$ 的实振幅部分并进行归一化操作, 即可解密出隐藏的实振幅图像 f' 为

$$\begin{aligned} &f'(x_{\rm o},y_{\rm o}) \\ =& \frac{\mathrm{abs}(wU_{\rm o}) - \min[\mathrm{abs}(wU_{\rm o})]}{\max[\mathrm{abs}(wU_{\rm o})] - \min[\mathrm{abs}(wU_{\rm o})]}, \end{aligned} \tag{6}$$

其中, abs() 代表取实振幅操作, max() 和 min() 分别取最大值和最小值操作.

3 软件设计

我们主要采用基于 Matcom 的 Visual C++ 与 Matlab 混合编程设计模式来设计所提出的光学信息隐藏软件. Matcom 软件平台本身的功能相当强大, 作为基于 Matrix 的一个编译器, 它可将 Matlab 的源代码译成同等功能的 C++ 源代码. 因此它既保持了 Matlab 的优良算法, 又保持了 C++ 的高执行效率 [17,18].

3.1 软件的基本设计思路

基于相移干涉术的信息隐藏系统软件所要完成的主要功能模块有: 1) 图像数据的读取、显示. 要求软件可方便地将图像数据格式化为二维矩阵格式保存在内存中. 为了方便调用, 将图像文件读取到系统内存中并显示到屏幕上. 2) 基于三步相移干涉的数字图像加密. 要求软件能够自主产生随机相位板, 并能够根据提供的波长、距离等几何参数, 实现对数字图像的加密并显示. 3) 水印嵌入. 要求软件能够根据用户输入的权重因子, 将水印嵌入到宿主图像中并显示. 4) 隐藏信息提取及解密. 要求软件能够利用 2) 中自主产生的随机相位板, 以及提供的波长、距离等参数, 实现对数字图像的提取、解密和显示, 而且能够给出解密图像的评价参数. 5) 攻击测试. 要求软件能够提供攻击模式选择功能, 能够根据用户输入的攻击参数对嵌入水印的图像进行攻击并显示; 能够对解密的数字图像进行滤波操作以提高提取水印的图像质量.

基于以上功能模块设计思想, 设计的信息隐藏软件采用 Microsoft 公司的 Visual C++ 作为基础开发平台, 使用其集成的 MFC (Microsoft Foundation Classes) 框架开发程序基本结构作为软件的交互界面 [17,18]; 涉及数字图像处理的部分采用 Matlab 转 C++ 函数的形式进行调用, 混合编程实现软件的设计. 设计的软件应具备以下特点: 1) 使用 Windows 运行环境, 具有与 Windows 程序风格相同的程序框架结构; 2) 良好的交互界面, 程序操作直观简洁; 3) 相对较快的运行速度, 能够实时完成数字水印的嵌入和提取以及攻击测试等; 4) 程序代码管理合理、移植方便, 程序具有较高的可维护性和安全保密性.

3.2 软件系统的基本结构

MFC 是用来编写 Windows 应用程序的 C++ 类集, 该类集以层级结构组织起来, 其中封装了大部分 Windows API 函数和 Windows 控件, 它所包含的功能涉及到整个 Windows 操作系统. MFC 不仅为用户提供了 Windows 图形环境下应用程序的框架, 而且还提供了创建应用程序的组件 [17,18]. 利用 MFC 和向导 (Wizard) 来编写 Windows 应用程序时, 首先使用 Class Wizard 来生成 Windows 应用程序的基本框架, 然后用 Class Wizard 来建立应用程序的类、消息处理、数据处理函数或定义控件的属性、事件和方法, 最后把各应用程序所要求的功能添加到类中.

基于设计软件应具有界面简洁、美观、操作简单等方面考虑, 软件的信息隐藏应用程序采用 MFC 提供的对话框 (Dialog) 类设计实现, 软件设计的基本系统结构框图如图 2 所示. 定义一个 CDialog 派生类的对话框类与资源相连接, 并在这个对话框类中定义一些成员变量与对话框中的控件相对应, 对话框类的函数成员负责对话框的打开与关闭、数据的传递等, 分别实现对宿主图像、水印图像的读取以及水印的嵌入、提取等操作.

3.3 软件操作界面

我们设计和开发出的光学信息隐藏软件的部分运行界面如图 3—5 所示. 图 3 为该软件运行时基本的图像信息加密及嵌入界面, 通过此界面, 可以实现几何参数、权重因子、原始水印图像和宿主图像的输入与显示, 以及水印图像信息的加密及嵌入等功能; 图 4 为该软件抗裁剪攻击时的运行界面, 输入裁剪攻击参数后, 可以完成其鲁棒性测试工作, 最后显示出最终滤波后的提取水印图像, 并计算出其相关系数; 与图 4 类似, 图 5 为该软件抗噪声攻击时的运行界面, 通过此界面, 可以完成高斯噪声、椒盐噪声和散斑噪声的抗攻击测试工作; 对比测试表明, 当采用相似的噪声攻击参数时, 系统抗椒盐噪声攻击的鲁棒性最好, 抗散斑噪声攻击的鲁棒性次之, 抗高斯噪声攻击的鲁棒性最差.

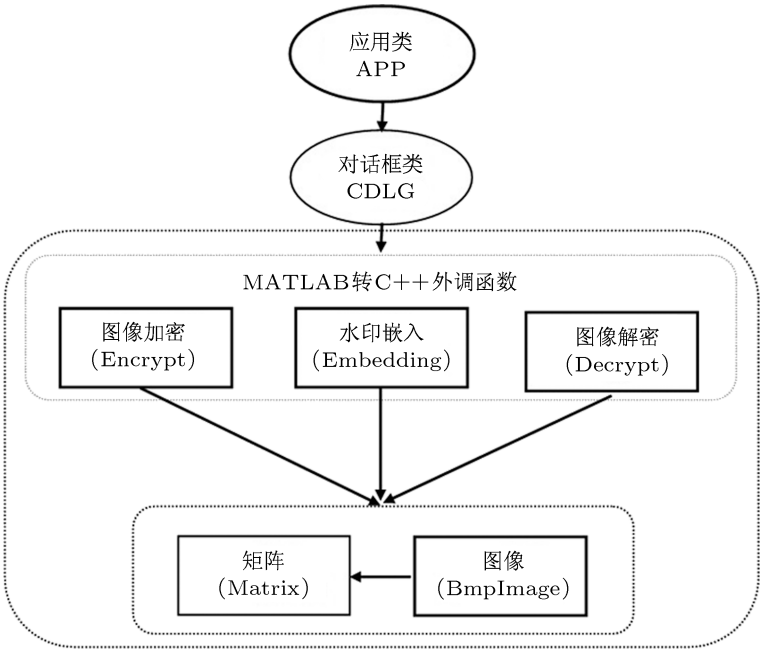

图 2 软件设计的基本系统结构框图

图 3 软件的图像信息加密及嵌入界面

图 4 软件的抗裁剪攻击测试界面

图 5 软件的抗噪声攻击测试界面

4 结 论

结合菲涅耳域的双随机相位编码技术, 本文提出了一种基于相移干涉术的信息加密及隐藏方案, 并进行了系统的软件设计与开发. 信息隐藏系统软件主要通过基于 Matcom 的 Visual C++ 与 Matlab 混合编程来实现, 它采用面向对象的设计模式和管理模块化的设计思想, 具有扩展性好、可靠性高、易于维护等优点. 而且, 采用 Visual C++ 开发环境可以实现友好的用户界面、功能齐全的执行模块以及规范化的接口. 所开发的信息隐藏软件可以很好地完成图像读取及显示、基本几何参数输入、信息嵌入及加密、信息提取及解密、鲁棒性测试等主要功能.

[1] Refrégier P, Javidi B 1995 *Opt. Lett.* **20** 767

[2] Javidi B 2005 *Optical and digital techniques for information security* (New York: Springer)

[3] Chang H T, Lu W C, Kuo C J 2002 *Appl. Opt.* **41** 4825

[4] Nomura T, Uota K, Morimoto Y 2004 *Opt. Eng.* **43** 2228

[5] Liu Z J, Liu S T 2007 *Opt. Commun.* **275** 324

[6] Yuan S, Zhou X, Li D H, Zhou D F 2007 *Appl. Opt.* **46** 3747

[7] Zhou N R, Wang Y X, Gong L H, He H, Wu J H 2011 *Opt. Commun.* **284** 2789

[8] Peng X, Tang H Q, Tian J D 2007 *Acta. Phys. Sin.* **56** 2629 (in Chinese) [彭翔, 汤红乔, 田劲东 2007 物理学报 **56** 2629]

[9] Liu F M, Zhai H C, Yang X P 2003 *Acta. Phys. Sin.* **52** 2462 (in Chinese) [刘福民, 翟宏琛, 杨晓苹 2003 物理学报 **52** 2462]

[10] Javidi B, Nomura T 2000 *Opt. Lett.* **25** 28

[11] Yamaguchi I, Zhang T 1997 *Opt. Lett.* **22** 1268

[12] Cai L Z, He M Z, Liu Q, Yang X L 2004 *Appl. Opt.* **43** 3078

[13] Meng X F, Cai L Z, He M Z, Dong G Y, Shen X X 2005 *J. Opt.* A: *Pure Appl. Opt.* **7** 624

[14] Meng X F, Cai L Z, Xu X F, Yang X L, Shen X X, Dong G Y, Wang Y R 2006 *Opt. Lett.* **31** 1414

[15] Meng X F, Cai L Z, Yang X L, Xu X F, Dong G Y, Shen X X, Zhang H, Wang Y R 2007 *Appl. Opt.* **46** 4694

[16] Meng X F, Peng X, Cai L Z, He W Q, Qin W, Guo J P, Li A M 2010 *Acta. Phys. Sin.* **59** 6118 (in Chinese) [孟祥锋, 彭翔, 蔡履中, 何文奇, 秦琬, 郭继平, 李阿蒙 2010 物理学报 **59** 6118]

[17] Consularo L A, Costa L 1998 *Comput. Phys.* **12** 460

[18] Qin W X, Liu J Y, Zhao W, Wang S H 2007 *J. Syst. Eng. Electron* **29** 795 (in Chinese) [钱伟行, 刘建业, 赵伟, 汪叔华 2007 系统工程与电子技术 **29** 795]

Software realization of optical information hiding system based on phase-shifting interferometry*

Fan De-Sheng[1)] Meng Xiang-Feng[1)†] Yang Xiu-Lun[1)] Wang Yu-Rong[1)]
Peng Xiang[2)] He Wen-Qi[2)]

1) (*Department of Optics, School of Information Science and Engineering and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Jinan* 250100, *China*)

2) (*College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, Shenzhen University, Shenzhen* 518060, *China*)

(Received 27 May 2012; revised manuscript received 15 June 2012)

Abstract

Combining the techniques of double random phase encoding and phase-shifting interferometry, an information hiding system is proposed, in which the information to be hidden can be encrypted into multiple interferograms. By choosing the appropriate weighting factor, the interferograms can be embedded in the host image. The secrete information can be successfully extracted and decrypted by special phase-shifting reconstruction formula and inverse Fresnel diffraction transform. A software of information hiding system is designed by mixed programming between Visual C++ and Matlab based in the Matcom software environments. By testing the software interface, the designed software can successfully realize the main functions, such as image reading and displaying, input of basis geometrical parameters, information encrypting and embedding, information extracting, decrypting, robustness testing, etc..

Keywords: image encryption and digital watermarking, phase-shifting interferometry, digital image processing

PACS: 42.40.Kw, 42.87.Bg, 07.05.Pj, 42.30.Rx

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60907005, 61171073, 61275014), the Natural Science Foundation of Shandong Province (Grant No. ZR2011FQ011), the Science and Technology Programs of Shandong Province (Grant No. 2011GGH20119), the Research Award Fund for Outstanding Young Scientists of Shandong Province (Grant No. BS2011DX023), the Science & Technology Bureau of Shenzhen (Grant No. 0014632063100426032), and the Independent Innovation Foundation of Shandong University (Grant No. IIFSDU, 2010TB019).

† E-mail: xfmeng@sdu.edu.cn