傅里叶变换全息加密数字水印解密实验研究

张雷洪[1]，孙刘杰[1]，郑继红[1]，马秀华[2]
(1. 上海理工大学，上海 200093；2. 中国科学院 上海光学精密机械研究所，上海 201800)

摘要：在理论分析傅里叶变换加密全息水印技术的基础上，通过 MATLAB 软件对加密全息水印的生成和提取进行了模拟仿真，验证了加密全息水印技术的安全性。通过搭建的光学解密再现系统，对经过计算机滤波处理后的含水印载体图像进行了光学解密再现，结果表明，无需原始载体图像的参与，通过正确的密匙就可以提取出原始水印图像，验证了加密全息水印技术的抗攻击性。对不同嵌入强度、位压缩、剪切、嵌入白噪声的载体图像进行了解密实验，计算其 PSNR，得到了 PSNR＞20，即加密全息水印具有较强的抗低通滤波、噪声、剪切性能，具有较强的鲁棒性。傅里叶变换加密全息水印解密光学系统相对于计算机仿真系统，具有高并行性、高处理速度、高信息维度、便捷性等优点，可用于进行版权保护。

关键词：傅里叶变换；加密水印；全息
中图分类号：TS853^{+}.6 **文献标识码**：A **文章编号**：1001-3563(2011)17-0008-05

Experiment Study on Decryption of Fourier Transform Holography Encrypted Watermark

ZHANG Lei-hong[1], *SUN Liu-jie*[1], *ZHENG Ji-hong*[1], *MA Xiu-hua*[2]
(1. University of Shanghai for Science and Technology, Shanghai 200093, China; 2. Shanghai Institute of Optics and Fine Mechanics, Shanghai 201800, China)

Abstract: The generation and extraction process of holography encrypted watermark was simulated by MATLAB software, based on theoretical analysis of Fourier transform holography encrypted watermark. The security of the watermark was proved. The carrier image processed by computer filter and carried the watermark was decrypted by optical decrypted reconstruction system. The original watermark image can be obtained by the right key without the original carrier image. The anti-attack property was tested by the decryption experiment. The original watermark was recovered from the watermarked images distorted by noise added, JPEG compression, part occluded, and low pass filter. The PSNR was computed to be bigger than 20. So the holography encrypted watermark has a good robustness. The optical decrypted reconstruction system has a higher parallelity, processing speed, information dimensions, convenient than the computer simulation system. It can be used for copyright protection.

Key words: Fourier transform; encrypted watermark; holography

随着计算机技术的迅猛发展和信息化建设步伐的加快，人们广泛地使用数字设备来制作、处理、传输和存储各种多媒体数字作品。数字作品给人们带来便利的同时，也产生了数字信息化传输的安全性控制和数字作品的版权保护等一系列问题。数字水印是实现版权保护的有效方法，如今已成为多媒体信息安全研究领域的一个热点。文献[1－14]对数字水印的光全息加密进行研究，提出了傅里叶变换全息加密技术；文献[1]通过搭建的光学加密系统对傅里叶变换全息加密进行光学实验研究，验证了加密的可行性。

收稿日期：2011-06-10
基金项目：上海理工大学博士启动费(1D-11-309-001)；上海市 085 工程项目资助；上海市教委重点课程(1K-11-309-001)；上海理工大学核心课程(1K-00-309-007)
作者简介：张雷洪(1981－)，男，江苏泰兴人，博士，上海理工大学讲师，主要从事数字水印研究。

由于傅里叶变换全息加密系统的输入相位调制模板和密匙调制模板存在对不准的问题,以上文献的研究,只给出了一个单相位加密调制的实验结果,没有对光学解密再现实验进行研究。笔者在理论分析傅里叶变换全息加密、解密的基础上,通过搭建的光学解密系统对嵌入傅里叶变换全息加密数字水印的载体图像进行光学解密实验,验证数字水印的版权保护认证的可行性以及光学系统的并行性和快捷性,并通过对比试验验证傅里叶变换全息加密水印的鲁棒性和安全性。

1　傅里叶变换全息加密技术

傅里叶变换全息加密技术融合双随机加密技术和全息技术,是一种新的加密技术。傅里叶变换加密全息图只有在密钥参与下,才能解密获得原始图像,具有较高的安全性,可用于版权保护和认证。

1.1　傅里叶变换全息加密过程

傅里叶变换全息加密采用 Mach-Zehnder 干涉仪结构。待加密原始图像 $f(x,y)$在加密光学系统输入平面上经过随机加密相位模板 $\alpha(x,y)$调制后,通过傅里叶变换透镜进行傅里叶变换,再由放置在傅里叶变换透镜输出频谱面上的随机相位模板 $B(\xi,\eta)$进行调制。这样经过双随机相位加密模板调制的物光与参考光 $R(\xi,\eta)$进行叠加干涉,就得到傅里叶变换加密全息图 $I_E(\xi,\eta)$。$I_E(\xi,\eta)$通过计算功率谱去除常数项后,得到最终的傅里叶变换加密全息图 $I_E'(\xi,\eta)$[1]:

$$I_E'(\xi,\eta)=\{[F(\xi,\eta)\otimes A(\xi,\eta)]B(\xi,\eta)\}R^*(\xi,\eta)+\{[F(\xi,\eta)\otimes A(\xi,\eta)]B(\xi,\eta)\}*R(\xi,\eta) \quad (1)$$

式中:$F(\xi,\eta)$和 $A(\xi,\eta)$分别表示 $f(x,y)$和 $\alpha(x,y)$的傅里叶变换;符号⊗表示卷积运算。

密匙 $B(\xi,\eta)$的全息图 $K(\xi,\eta)$通过计算功率谱去除常数项后,得到傅里叶变换加密全息图的解密密钥的全息图 $K'(\xi,\eta)$[1]:

$$K'(\xi,\eta)=B(\xi,\eta)R^*(\xi,\eta)+B^*(\xi,\eta)R(\xi,\eta) \quad (2)$$

1.2　傅里叶变换加密全息解密过程

将加密的傅里叶变换全息图和密钥全息图相乘[1]:

$$I_E'(\xi,\eta)\times K'(\xi,\eta)=\{[F(\xi,\eta)\otimes A(\xi,\eta)]B(\xi,\eta)\}R^*(\xi,\eta)[B^*(\xi,\eta)R(\xi,\eta)]+\{[F(\xi,\eta)\otimes A(\xi,\eta)]\cdot B(\xi,\eta)\}R^*(\xi,\eta)[B(\xi,\eta)R^*(\xi,\eta)]+\{[F(\xi,\eta)\otimes A(\xi,\eta)]B(\xi,\eta)\}R^*(\xi,\eta)[B(\xi,\eta)R^*(\xi,\eta)]+\{[F(\xi,\eta)\otimes A(\xi,\eta)]B(\xi,\eta)\}R^*(\xi,\eta)[B^*(\xi,\eta)R(\xi,\eta)] \quad (3)$$

通过式(3)中第 1 项和第 2 项的傅里叶变换,就可直接解密提取出原始图像 $f(x,y)$和其共轭图像 $f^*(x,y)$;第 3 项和第 4 项是随机噪声信号。

2　傅里叶变换加密全息水印

2.1　加密全息水印

傅里叶变换加密全息水印技术可分成水印的生成、水印的嵌入和水印的提取 3 个过程。

2.1.1　加密全息水印生成

傅里叶变换加密全息水印是通过傅里叶变换加密全息技术生成的。通过傅里叶变换全息生成的加密全息图像,记作 $H'(x,y)$,其函数值是实数值,而且由于经过双随机调制,所以是随机分布的。

2.1.2　加密全息水印嵌入和提取

设 $C(x,y)$表示载体图像,$I(x,y)$表示含水印的载体图像,$H'(x,y)$是加密水印信息,α 表示嵌入系数。含水印的载体图像 $I(x,y)$[4]:

$$I(x,y)=\alpha H'(x,y)+C(x,y) \quad (4)$$

原始图像的解密提取过程为:首先将 $I(x,y)$与解密密钥的全息图进行相乘,再经过一次傅里叶变换就可提取得到原始图像 $f(x,y)$。其中 $I(x,y)$为实值函数图像。

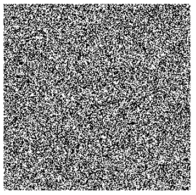
2.2　全息水印的嵌入和提取仿真

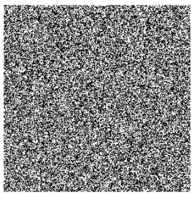
通过对傅里叶变换加密全息算法的研究,采用 MATLAB 软件进行仿真。对原始图像 $f(x,y)$进行 $\alpha(x,y)$调制后进行傅里叶变换,再进行随机加密相位模板 $B(\zeta,\eta)$的调制,最后生成傅里叶变换加密全息图像。按嵌入系数 α,对载体图像 $C(x,y)$和傅里叶变换加密全息图进行叠加求和生成嵌入全息水印的载体图像。嵌入加密水印后的载体图像见图 1e,可见载体图像看不出水印的痕迹,体现了水印的不可见性。

加密全息水印的提取过程:对嵌入加密水印后的图像进行滤波处理;滤波处理后载体图像与随机加密相位模板 $B(\zeta,\eta)$全息图像相乘,再进行傅里叶变换就可以得到原始水印图像 $f(x,y)$。解密提取过程不需要原载体图像的参与,属于盲提取技术。解密提取出的原始水印图像(图 1h)与原始水印(图 1b)相似。

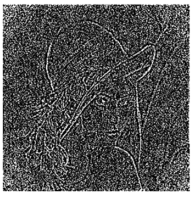

a 原载体图像

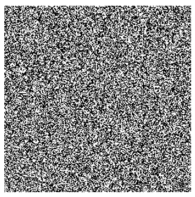
b 水印图像


c 傅里叶变换加密全息水印


d 密匙全息图


e 嵌入加密水印后图像


f 图e进行滤波后图像


g 密匙全息图d与图f相乘

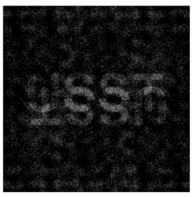

h 从图g中提取的水印图像

图 1 加密全息水印的嵌入和提取

Fig. 1 Embedding and extracting of the encrypted watermarked image

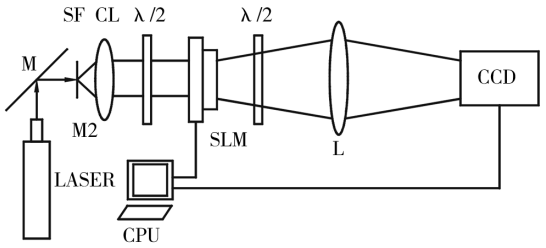
3 傅里叶变换加密全息水印解密再现实验

在傅里叶变换加密全息水印的加密实验中,由于2块调制的相位模板存在对不准的问题,文献[1]用傅里叶变换透镜来代替密匙相位模板进行实验。由于密匙过于简单,安全性较差,不能体现实验的一般性;解密时也同样存在密匙全息与加密全息图对不准的问题。采用计算机模拟得出的傅里叶变换加密全息水印进行水印的提取再现实验,验证水印的安全性和鲁棒性。

采用氦氖激光器,波长 632.8 nm;傅里叶变换透镜,焦距 300 mm,口径 50.8 mm;宽带分光棱镜;AVT 数字摄像机,像素 1 628×1 236,14 fps,1/1.8" CCD,Gige/1394 接口;德国 HOLOEYE 公司生产的空间光调制器 LC2002 SLM(spatial light modulator),中间面积为 26.6 mm×20.0 mm,90°扭曲向列型投射液晶,显示分辨率为 800×600,像素大小为 32 μm×32 μm 等,搭建光学解密再现系统,见图 2。

3.1 傅里叶变换加密全息水印解密再现实验

加密全息水印解密实验采用图 2 所示的水印重



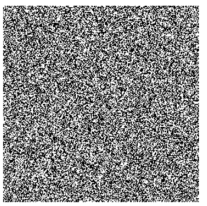
M—反射镜;SF—小孔滤波;CL—准直透镜组;SLM—空间光调制器;L—傅里叶变换透镜

图 2 傅里叶变换加密全息图解密再现的光路系统

Fig. 2 Optical decrypted reconstruction system

建光学实验系统。实验步骤如下:(1)按图 2 组建实验系统,调整光阑,使出射光成为光斑直径大于 30 mm 的平行光束;(2)连接 SLM 和 CCD 到计算机系统,将 SLM、透镜 L 和 CCD 同轴安放在光路上,并使 SLM 和 CCD 分别位于透镜的前后频谱面上;(3)将滤波处理后的含水印图像与解密密钥全息图相乘的结果显示在 SLM 上,调整 SLM 和 CCD 相关参数,就可以得到提取的水印图像。实验结果见图 3。

a 原始水印图像


b 嵌入水印后图像与密匙全息图相乘

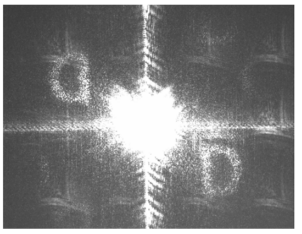

c 实验提取的水印图像

图 3 加密傅里叶变换全息水印的嵌入和提取

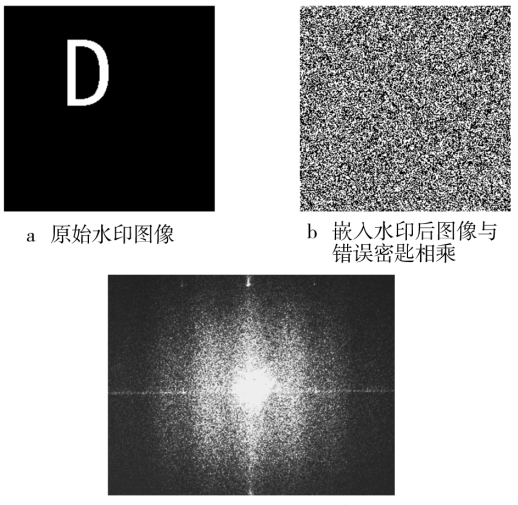
Fig. 3 Embedding and extracting of the encrypted watermarked image

从图 3 可知,水印解密光学实验系统提取的水印图像与原始水印图像相似,包含有原始水印和其共轭图像。由于傅里叶变换透镜频谱面位置误差和空间光调制器的对准问题,提取的水印图像的轮廓模糊。

3.2 采用错误的密匙全息图进行再现实验

加密傅里叶变换全息水印嵌入和采取错误的密

匙提取的结果见图 4,错误的密匙全息与嵌入加密全



a 原始水印图像　b 嵌入水印后图像与错误密匙相乘　c 实验提取的水印图像

图 4　加密傅里叶变换全息水印的嵌入和采取错误的密匙提取

Fig. 4 Embedding and extracting of the encrypted watermarked image with wrong key

息水印后的载体图像相乘后,无法通过图 2 的水印重建光学实验系统提取出原始水印,验证了加密全息水印的安全性和抗攻击性。

3.3　傅里叶变换加密全息水印的鲁棒性实验

由于全息图受均值为零,方差为 σ 的高斯随机噪声干扰,实验提取的原始图像的效果比较差。采用解密图像的峰值信噪比 PSNR[15-20] 来比较实验中提取水印图像的效果:

$$\mathrm{PSNR}=10\lg\frac{MN}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}[f(x,y)-\tilde{f}(x,y)]^2} \quad (5)$$

式(5)中:$f(x,y)$ 和 $\tilde{f}(x,y)$ 分别为含水印载体图像中提取的水印图像和直接由傅里叶变换加密全息图提取的水印图像;M,N 为图像的像素值。

3.3.1　嵌入强度系数变化

改变嵌入系数 α,得到嵌入加密水印强度不同的含水印载体图像,分别与密匙的全息图相乘后,送入图 2 的光学解密系统,提取出原始水印。按照式(5)计算不同嵌入系数下提取的原始水印图像的 PSNR。绘制不同嵌入强度下解密图像的峰值信噪比见图 5。

可见随着嵌入系数的增大,载体图像中嵌入水印的信息增大,实验提取的原始水印的 PSNR 增大,解密再现的原始水印图像效果变好。图 5 把采用 MATLAB 软件仿真获取的曲线与采用光学解密系统获取的曲线进行了比较,可见由于光学系统的非线性

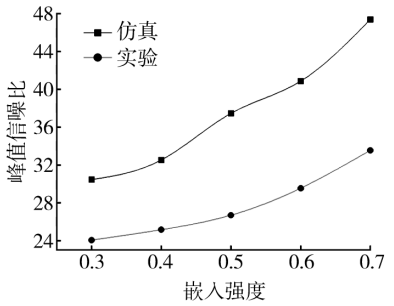


图 5　不同嵌入强度下解密图像的峰值信噪比

Fig. 5 The PSNR of the decrypted image in different embedding coefficient

以及光学元器件的精度影响,实验提取的原始水印图像较计算模拟提取的原始水印图像差。实验结果表明,傅里叶变换加密全息水印在嵌入强度较低的条件下,仍能提取出水印信息,具有较强的鲁棒性。

3.3.2　添加白噪声

在嵌入系数为 0.3 的含水印载体图像中添加 0.05～0.15 强度的随机白噪声,分别与密匙的全息图相乘后,送入图 2 的光学解密系统,提取出原始水印。按照式(5)计算不同白噪声嵌入系数下提取的原始水印图像的 PSNR。不同噪声条件下的解密图像的峰值信噪比见图 6。

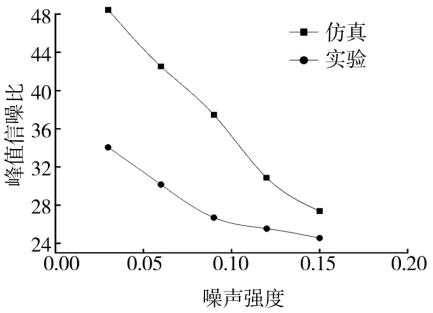


图 6　不同噪声条件下的解密图像的峰值信噪比

Fig. 6 The PSNR of the decrypted image in different noise

可见随着随机白噪声强度的增大,实验提取的原始水印的 PSNR 减小,解密再现的原始水印图像效果变差。实验提取的原始水印图像较计算模拟提取的原始水印图像差。在添加强度为 0.15 时,PSNR 依然大于 20,添加随机白噪声后的含水印图像仍能准确地提取出水印信息。可见,该水印算法对添加的随机噪声具有较强的鲁棒性。

3.3.3　部分剪切

将嵌入系数为 0.3 的含水印载体图像剪切掉其

中心的大部分,对剩余部分图像进行实验再现提取水印,提取水印图像的 PSNR 见图 7,可见随着剪切面

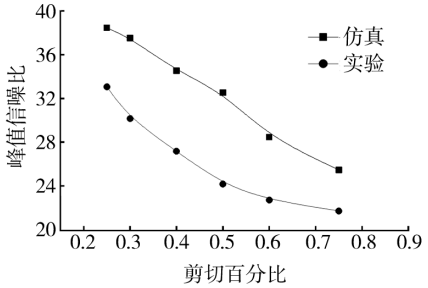


图 7 不同剪切条件下的解密图像的峰值信噪比

Fig. 7 The PSNR of the decrypted image in different part occluded

积的增大,实验提取的原始水印的 PSNR 减小,解密再现的原始水印图像效果变差。实验提取的原始水印图像较计算模拟提取的原始水印图像差。在剩余面积为 25%时,PSNR 依然大于 20,仍能准确地提取出水印信息,证明该加密全息水印的嵌入对剪切攻击具有较强的鲁棒性。

3.3.4 位压缩

将嵌入系数为 0.3 的含水印载体图像进行有损质量压缩,提取水印图像的 PSNR 见图 8,可见随着

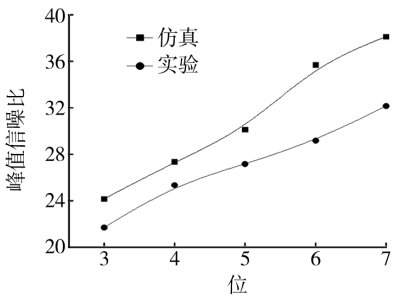


图 8 不同位压缩下的解密图像的峰值信噪比

Fig. 8 The PSNR of the decrypted image in different JPEG compression

图像位数的减小,实验提取的原始水印的 PSNR 减小,解密再现的原始水印图像效果变差。实验提取的原始水印图像较计算模拟提取的原始水印图像差。在图像位数为 3 时,PSNR 依然大于 20,仍能准确地提取出水印信息,证明加密全息水印的嵌入对位压缩具有较强的鲁棒性。

3.3.5 加密水印其余鲁棒性能实验

通过 Photoshop 画笔,对将嵌入系数为 0.3 的含水印载体图像严重涂鸦污染后进行水印提取,计算其 PSNR,PSNR=23.63。对嵌入系数为 0.3 的含水印载体图像进行高斯低通滤波,滤波器阶数 $N=2$,截止频率 $D_0=50$,其 PSNR=21.32。可见经过涂鸦和滤波后的载体图像,提取的水印具有较强的鲁棒性。通过实验还可以得出,该水印加密、嵌入、提取技术对于不同的载体图像和水印图像具有较强的适应性,并且能够在不需要原始载体信息的情况下较准确地提取原始水印。

由实验结果可见:双随机相位的傅里叶变换加密全息水印技术结合了光学加密技术、数字水印技术,具有较好的不可见性、安全性和鲁棒性。实验证明了傅里叶变换加密全息水印具有较强的抗低通滤波、噪声、剪切和对不同载体图像和水印信息的适应性,不需要原始载体图像的参与,可以直接提取出原始水印。光学解密再现系统验证了傅里叶变换加密全息水印的安全性,鲁棒性。同时,光学系统相对于计算机模拟系统具有高并行性、高处理速度、高信息维度、便捷性等优点。

4 结论

在理论分析傅里叶变换加密全息水印的基础上,通过 MATLAB 软件对加密全息水印的生成和提取进行了计算机模拟仿真。验证了加密全息水印技术无需原始载体图像的参与,可直接提取出原始水印,具有较强的安全性,可用于版权保护。

参考文献:

[1] JAVIDI B, NOMURA T. Securing Information by Use of Digital Holography[J]. Opt Lett, 2000, 25(1): 28-30.

[2] NISHCHAL N K, JOSEPH J, SINGH K. Fully Phase Encryption Using Digital Holography[J]. Opt Eng, 2004, 43(12): 2959-2966.

[3] XU L, PENG X, GUO Z, et al. Imaging Analysis of Digital Holography[J]. Opt Express, 2005, 13(7): 2444-2452.

[4] TAKAI N, MIFUNE Y. Digital Watermarking by a Holographic Technique[J]. Appl Opt, 2002, 41(5): 865-873.

[5] KISHK S, JAVIDI B. 3D Watermarking by a 3D Hidden Object[J]. Opt Express, 2003, 11(8): 874-888.

(下转第 16 页)

5 分析总结

首先，创新地将网络印刷服务引入了智能手机这一携带率最高的移动设备，符合办公、娱乐、消费日益网络化、移动化的趋势，必将为网络印刷开拓新的市场。其次，本设计充分考虑了智能手机终端的特点，采用了操作简单的基于模版的产品设计服务方案，使用户在模版的基础上编辑自己的个性化作品，增加了产品的适用性。而对于基于模版的产品设计服务方案带来的一系列问题，创新地为每一个模版准备了高、低分辨率 2 份文件，高分辨率的模版存储在服务器空间，低分辨率模版下载到手机端供显示和编辑，输出时调用服务器中相应的高分辨率模版，使得在该方案中，智能手机端的模板浏览具有本地浏览的流畅感受，避免了在线浏览会因网络速度不佳导致页面更新速度过慢的情况，和大量信息传输带来的高能耗，同时又降低了数据量，避免了本地浏览方式导致的大量模版占用大量存储空间的问题。此外，该方案选取 XML 语言来记录编辑信息，XML 语言允许自定义标签，使用灵活且易于解析，因此可以相对容易地编写解析器，对其进行读写操作，其交换数据的能力也非常强大，可以便捷准确地为同样基于 XML 的 JDF 流程软件提供信息。总之，本设计在充分考虑智能手机终端的特点与通过手机进行的网上消费的特点，通过合理的设计与技术手段，使得该系统易于使用。

参考文献：

[1] 孔玲君. 网络印刷及其相关支持技术[J]. 数码印刷，2010(2)：21－23.

[2] 郑爱玲. 国内网络印刷发展现状调查[J]. 市场参考，2010(10)：14－16.

[3] 毛志娟，刘真，朱明. 基于 Kodak Insite 的网络印刷模型研究[J]. 包装工程，2010，31(19)：1－5.

[3] VistaPrint[OL]. http://www.vistaprint.com.au/vp/welcome.aspx? xnav=welcomeback&rd=2.(余不详)

[5] 季永芹. OPI 技术全接触[J]. 印刷杂志，2004(7)：1－3.

[6] 王克蒙，郑家农. JDF 文件基本结构分析[J]. 北京印刷学院学报，2007(6)：1－4.

[7] MOON Jongbae，KWAK Donggyu，CHI Yongyun，et al. A XML Script-Based Testing Tool for Embedded Softwares[M]. Computational Science and Its Applications － ICCSA，2007.

[8] 张惠文. 基于 XML 的元数据架构[J]. 现代情报，2002(7)：1－2.

(上接第 12 页)

[6] KISHK S，JAVIDI B. Information Hiding Technique with Double Phase Encoding [J]. Appl Opt，2002，41(26)：5462－5470.

[7] 彭翔，张鹏，牛憨笨. 虚拟光学信息隐藏理论及并行硬件实现[J]. 光学学报，2004，24(5)：623－627.

[8] NOMURA T，OKAZAKI A，KAMEDA M，et al. Image Reconstruction from Compressed Encrypted Digital Hologram[J]. Opt Eng，2005，44(7)：5801－5807.

[9] KIM H，KIM D H，LEE Y H. Encryption of Digital Hologram of 3-D Object by Virtual Optics[J]. Opt Express，2004，12(20)：4912－4921.

[10] CHENG C J，LIN L C. Correlation-based Watermarking by a Digital Holographic Technique[J]. Opt Eng，2005，44(1).(余不详)

[11] ABOOKASIS D，MONTAL O，ABRAMSON O，et al. Watermarks Encypted in a Concealogram and Deciphered by a Modified Joint-transform Correlator[J]. App Opt，2005，44(15)：1－5.

[12] KIM H，LEE Y H. Optical Watermarking of Digital Hologram of 3-D Object[J]. Opt Express，2005，13(8)：2881－2886.

[13] KISHK S，JAVIDI B. 3D Watermarking by a 3D Hidden Object[J]. Opt Express，2003，11(8)：874－888.

[14] FRANEL Y，CASTRO A，NAUGHTON T J，et al. Security Analysis of Optical Encryption[J]. Proc of SPIE 2005，5986：25－34.

[15] Van DROOGENBROECK M，BENEDETT R. Techniques for a Selective Encryption of Uncompressed and Compressed Images[J]. In ACIVS02，Ghent，Belgium，2002 Proceedings of Advanced Concepts for Intelligent Vision Systems，2002：90－97.

[16] 林睿，常鸿森，李榕. 光学图像识别相关器的 MATLAB 仿真[J]. 华南师范大学学报，2004，4(11)：70－73.

[17] 黄军. 基于离散余弦变换域的数字水印研究[J]. 包装工程，2010，31(13)：108－110.

[18] 丁盈盈，刘真. 3 种频域数字水印算法的分析和比较[J]. 包装工程，2011，32(5)：103－107.

[19] 黄惠芬. 分形与小波相结合的鲁棒性数字水印算法[J]. 包装工程，2010，31(11)：31－33.

[20] 王灿才. 基于空间域 LSB 数字水印的鲁棒性研究[J]. 包装工程，2009，30(3)：76－78.