

文章编号: 0253-2239(2009)10-2709-07

基于级联分数傅里叶变换系统的数字水印技术

赫明钊 曹良才 谭峭峰 何庆声 金国藩

(清华大学精密仪器与机械学系,精密测量技术与仪器国家重点实验室,北京 100084)

摘要 提出一种基于分数傅里叶变换和随机相位编码的光学加密数字水印技术,可成为一种信息隐藏及保护的有效方案。该数字水印技术对于噪音叠加和常见的图像处理操作具有较强的稳健性。该技术根据光学级联分数傅里叶变换系统,利用两个随机相位分布函数对水印信息编码并经过迭代分数傅里叶变换嵌入到变换域的载体图像中。在水印检测和提取过程中,两个相位分布函数作为密钥。随机相位编码技术的引入,进一步提高了数字水印系统的密钥空间,增强了系统的安全性。该数字水印技术基于光学分数傅里叶变换原理,可以利用光学变换系统方便地实现。

关键词 傅里叶光学;数字水印;信息隐藏;随机相位编码

中图分类号 O438.2 **文献标识码** A **doi**: 10.3788/AOS20092910.2709

Digital Watermarking Technique Based on Cascaded Fractional Fourier Transform System

He Mingzhao Cao Liangcai Tan Qiaofeng He qingsheng Jin Guofan

(State Key Laboratory of Precision Measurement Technology and Instruments,

Department of Precision Instruments and Mechnadogy, Tsinghua University, Beijing 100084, China)

Abstract A novel digital watermarking method by optical cascaded fractional Fourier transform and random phase encoding is proposed. This method can be served as an effective way of information hiding and protection. Experimental results show that this watermarking method has strong robustness against noise, shearing, rotation, resizing, and medium filtering. This watermarking method is based on optical cascaded fractional Fourier transform system. The watermark information is iterative fractional Fourier transformed and embedded into host image. And two phase distributions can be obtained as keys to protect the watermark information. With the introduction of double phase encoding, the key space of this watermark system is greatly enlarged. As a result the security of this watermark system is enhanced. This watermark technique can be implemented both optically and digitally.

Key words Fourier optics; digital watermark; information steganography; random phase encoding

1 引 言

数字水印作为一种解决数字产品版权问题的有效手段,近年来得到了人们的广泛关注,并逐渐成为多媒体数据安全领域的一个研究热点^[1~8],也是信息隐藏技术研究领域的重要分支。一个有效的数字水印技术必须具备一些基本特征:视觉不可见性、稳健性、和安全性^[2]。已报道的大部分数字水印技术达到

了较好的视觉不可见性和稳健性,然而水印算法的安全性未充分考虑,按照密码学的“Kerckhoffs 假设”将水印算法公开,则隐藏的水印信息易被破解。加密技术^[9~13]虽然具有较高的安全性,但由于密文的特殊性,易成为攻击的对象。因此本文结合加密技术和数字水印,提出一种安全性极高的数字水印技术,同时也是一种具有较好的隐蔽性的加密技术。

收稿日期: 2008-12-19; **收到修改稿日期**: 2009-01-15

基金项目: 国家自然科学基金(60677037,60807005)资助项目。

作者简介: 赫明钊(1980—),男,博士研究生,主要从事光学信息处理方面的研究。

E-mail: hemz05@mails. tsinghua. edu. cn

导师简介: 金国藩(1929—),男,中国工程院院士,主要从事计算全息、光计算及二元光学等方面的研究。

光学信息安全^[2, 13]采用光学信息处理原理和技术实现数字信息的加密和隐藏。与完全采用计算机和电子系统的信息安全技术相比,光学信息安全技术具有明显的优势,如高速并行性的处理能力,大容量,多维度的信息加密及解密能力。本文提出的数字水印技术基于级联光学分数傅里叶变换系统,即将水印信息经过迭代分数傅里叶变换及两次随机相位编码,嵌入到载体图像中;水印信息的提取可以采用数值计算或光学分数傅里叶变换系统方便实现。在迭代计算中,采用动态调制相位板的方法,在每次迭代运算中优化相位分布函数,达到了极好的收敛性。分数傅里叶变换及随机相位编码保证了水印信息均匀嵌入到载体图像中,实现了较好的视觉不可见性和稳健性。该数字水印技术引入了随机相位编码,得到两个随机相位分布作为密钥,无密钥和使用错误密钥均无法检测和提取水印,大大增强了其安全性和信息的隐藏性。该数字水印技术基于光学分数傅里叶变换原理,可以利用光学变换系统方便地实现。

2 迭代分数傅里叶变换

分数傅里叶变换(FRT)是传统的傅里叶变换在分数级次上的推广,与傅里叶变换有着紧密的联

系,又具有许多不同于傅里叶变换的特殊性质^[14~18]。如果设输入函数为 $f(x, y)$, 则其 P 级分数傅里叶变换的数学定义为

$$\mathcal{F}_P[f(x, y)] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) B(x, y; u, v; P) dx dy, \quad (1)$$

式中变换核函数为

$$B(x, y; u, v; P) = C_P \exp\{i\pi[(x^2 + y^2 + u^2 + v^2)\cos\varphi - 2(xu + yv)\csc\varphi]\}, \quad (2)$$

其中 C_P 为相位常数, $\varphi = P \cdot \pi/2$ 。二维分数傅里叶变换可以分解为沿着 x, y 方向的一个一维分数傅里叶变换^[13], 即 $B(x, y; u, v; P) = B_x(x, u; P) \cdot B_y(y, v; P)$ 。若 x, y 方向一维分数傅里叶变换的级次不同, 则称为分形分数傅里叶变换。1993 年 Lohmann 用正透镜实现了光学分数傅里叶变换^[17]。图 1 所示的光学系统即由两个光学分数傅里叶变换系统级联而成, 每个变换系统有四个参数。如第一级系统的参数有: 入射光波的波长 λ 、透镜的焦距 f_1 和输入及输出面到透镜的距离 d_1, d_2 , 其输入面到输出面的分数傅里叶变换表示为

$$g(u, v) = K \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y) \cdot \exp\left(i\pi \frac{a^2 x^2 + b^2 y^2}{\tan\alpha} - i2\pi \frac{abux}{\sin\alpha}\right) \cdot \exp\left(i\pi \frac{a^2 y^2 + b^2 v^2}{\tan\alpha} - i2\pi \frac{abvy}{\sin\alpha}\right) dx dy, \quad (3)$$

其中 a, b 和 α 可以用光学系统的参数得出^[18]。为了利用快速傅里叶算法(FFT)计算(3)式, 利用坐标代换得

$$g(u', v') = K' \exp\left[i\pi \frac{b\cos\alpha}{a}(u'^2 + v'^2)\right] \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x', y') \exp\left[i\pi \frac{a\cos\alpha}{b}(x'^2 + y'^2)\right] \cdot \exp[-i2\pi(x'u' + y'v')] dx' dy' = K' \exp\left[i\pi \frac{b\cos\alpha}{a}(u'^2 + v'^2)\right] \cdot \mathcal{F}_F^2\left\{f(x', y') \exp\left[i\pi \frac{a\cos\alpha}{b}(x'^2 + y'^2)\right]\right\}, \quad (4)$$

其中 $x' = x \sqrt{ab/\sin\alpha}, y' = y \sqrt{ab/\sin\alpha}, u' = u \sqrt{ab/\sin\alpha}, v' = v \sqrt{ab/\sin\alpha}$, \mathcal{F}_F^2 为二维快速傅里叶变换。根据光学系统的参数确定分数傅里叶变换的系数, 可以利用快速傅里叶变换算法实现非对称分数傅里叶变换的数值计算。

提出的数字水印算法基于级联分数傅里叶变换系统如图 1 所示, 输入域放置载体图像和相位密钥 key_1 , 中间域放置相位密钥 key_2 , 输出域为水印图像, 相邻域之间以分数傅里叶变换联系。为把水印图像嵌入到载体图像中, 需要迭代计算输入域的复振幅和中间域的相位分布。这类似一个相位恢复问

题。而迭代算法是相位恢复问题的常见解决方案, 它利用测量的物体的波前强度分布迭代计算物体的相位分布。迭代分数傅里叶变换算法就是结合分数傅里叶变换和迭代相位恢复算法, 由输出面的分数傅里叶面的幅值迭代计算输入面的强度及相位分

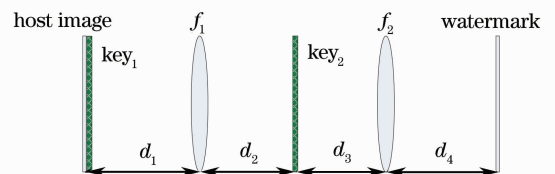


图 1 级联分数傅里叶变换系统

Fig. 1 Cascaded optical system of FRT

布。输入面到输出面的变换可以由非迭代数值计算或由光学分数傅里叶变换直接实现。

3 数字水印算法模型

提出的数字水印算法分为水印嵌入算法和水印提取算法两部分。

3.1 水印的嵌入

级联分数傅里叶变换系统如图 1 所示,系统结构参数有六个,波长为 λ 。设载体图像为 $h_0(x, y)$, 相位密钥 key_1 为 $k_1(x, y)$, 相位密钥 key_2 为 $k_2(u, v)$, 水印图像为 $w'(x', y')$ 。

水印的嵌入算法流程如图 2 所示,具体步骤为

1) 任意给出相位密钥 key_1 的初始值(相位在 0 到 2π 之间),与载体图像 $h_0(x, y)$ 相乘,构成输入域的复振幅函数 $h(x, y)$ 。做级次为 P_1 的二维分数傅里叶变换,得中间域的复振幅函数 $t(u, v)$;

2) 任意给出相位密钥 key_2 的初始值(相位在 0 到 2π 之间),与中间域的复振幅函数 $t(u, v)$ 相乘,再做级次为 P_2 的二维分数傅里叶变换得到输出域的复振幅函数 $w(x', y')$;

3) 引入约束条件 1(constraint 1):保持输出域的复振幅函数数 $w(x', y')$ 的相位部分不变,振幅用水印信息图像的平方根值 $\sqrt{w(x', y')}$ 代替;

4) 做级次为 P_2 的二维逆分数傅里叶变换,得到中间域的复振幅函数 $t'(u, v)$ 。除以相位密钥 key_2 ,再做级次为 P_1 的二维逆分数傅里叶变换,得到输入域的复振幅函数 $h'(x, y)$;

5) 根据一定判别条件判断第 n 次迭代的结果 $h'^{(n)}(x, y)$ 与载体图像的差别。若满足判别条件,则得出 $|h'^{(n)}(x, y)|$ 为嵌入水印信息的载体图像;若不满足条件,则引入约束条件 2(constraint 2):保持复振幅函数 $h'(x, y)$ 的相位部分不变,振幅用载体图像 $h_0(x, y)$ 和 $|h'(x, y)|$ 的线性组合代替,同时设定新的相位密钥 key_2 ,表示为

$$h^{(n+1)}(x, y) = [h_0(x, y) - \beta |h'^{(n)}(x, y)|] \exp\{i \cdot A[h'^{(n)}(x, y)]\}, \quad (5)$$

$$k_2^{(n+1)}(u, v) = N[t'^{(n)}(u, v)/t^{(n)}(u, v)], \quad (6)$$

式中 $A[\cdot]$ 为取幅角运算符, $N[\cdot]$ 为归一化操作。进行下一轮迭代,直到满足判别条件为止。强度因子 β 是一个常数,取值在 0 到 1 之间。

判别条件通常使用均方差或相关系数。为比较不同分辨率、不同灰阶图像的差别,引入归一化均方差(Normalized Mean-Squared Error)定量判别图像

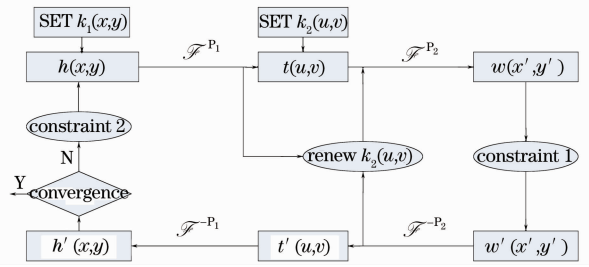


图 2 水印嵌入框图

Fig. 2 The Diagram of watermark embedding 的微小差别。

$$f_{\text{NMSE}} = \frac{\sum \sum [|h'^{(n)}(x, y) - h_0(x, y)|^2]}{\sum \sum [h_0(x, y)]^2}, \quad (7)$$

在迭代分数傅里叶变换计算中,设定一个阈值,当某次迭代计算得到 f_{NMSE} 小于此阈值,则停止迭代计算。也可用嵌入水印前后的载体图像相关系数作为判别条件,相关系数表示为

$$f_{\text{CC}} = \frac{f_{\text{COV}}(|h'|, h_0)}{\sigma_{|h'|} \sigma_{h_0}}, \quad (8)$$

$$f_{\text{COV}}(|h'|, h_0) = \frac{E[|h'| - E(|h'|)] E[h_0 - E(h_0)]}{E[h_0 - E(h_0)]}, \quad (9)$$

其中 f_{COV} 为协方差, $E[\cdot]$ 为数学期望。

本文用 MATLAB 语言进行编程实现了迭代分数傅里叶变换数字水印算法,载体图像和水印图像分辨率都是 $256 \text{ pixel} \times 256 \text{ pixel}$ 。级联分数傅里叶变换系统的参数为透镜 $f_1 = 100 \text{ mm}$, $d_1 = 60 \text{ mm}$, $d_2 = 80 \text{ mm}$, 透镜 $f_2 = 150 \text{ mm}$, $d_3 = 100 \text{ mm}$, $d_4 = 120 \text{ mm}$, 光波波长为 532 nm 。根据文献[18], $\alpha_1 = 1.2840$, $\alpha_2 = 1.0132$, 分数傅里叶变换级次 $P_1 = 0.8714$, $P_2 = 0.6450$ 。

本迭代算法具有较高的收敛效率。如图 3 所示,迭代运算进行到 5 次,归一化均方差接近于 0,而相关系数接近于 1。为保证更好的水印嵌入效果,在下面的所有实验中,迭代次数皆选为 10 次。

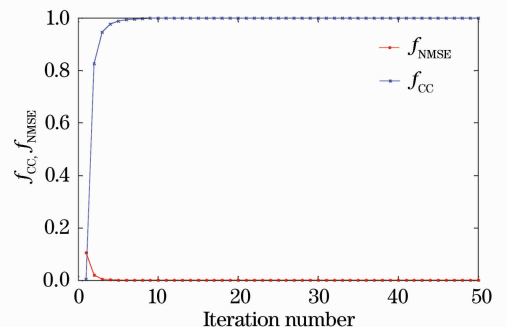


图 3 归一化均方差和相关系数收敛曲线

Fig. 3 f_{NMSE} and f_{CC} curves vs. iteration number

同时,本算法具有较快的运算速度,在 Intel(R) Pentium-IV 3.06 GHz 的计算机上模拟时,每次迭代运算仅需约 0.306 s。

3.2 水印的提取

水印信息的提取同样基于图 1 的级联分数傅里叶变换系统。由水印嵌入算法得到嵌入水印的图像为 $|h'(x, y)|$, 相位密钥 key_1, key_2 分别为 $k_1(x, y)$ 和 $k_2(u, v)$, 水印信息的提取可以用两次分数傅里叶变换迅速得出

$$t(u, v) = \mathcal{F}^1[|h'(x, y)|k_1(x, y)], \quad (10)$$

$$\omega(x', y') = |\mathcal{F}^2[t(u, v)k_2(u, v)]|^2, \quad (11)$$

水印提取的过程也可光学方便地实现,把嵌入水印的载体图像放在输入域,相位密钥 key_1, key_2 分别放置在输入域和中间域的准确位置上,特定波长的相干光照明,提取的水印就显示在输出域。

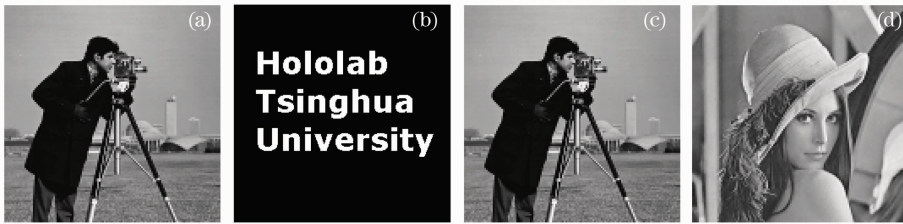


图 4 二值及灰阶水印嵌入及提取结果。(a)嵌入水印的载体图像;(b)提取的二值水印;
(c)嵌入水印的载体图像;(d)提取的灰阶水印

Fig. 4 Binary and gray-level watermark embedding and extraction. (a)host image;(b)extracted binary watermark;
(c)host image;(d)extracted gray-level watermark

4.1 视觉不可见性

嵌入二值和灰阶水印的载体图像分别为图 4(a)和(c)。从视觉效果看,人眼很难分辨出嵌入水印后的载体图像与原载体图像的差别。图像处理中通常使用峰值信噪比(Peak Signal to Noise Ratio, f_{PSNR})来量化嵌入水印后载体图像的质量。表 1 给出了 f_{PSNR} 与强度因子 β 的关系,实验表明, f_{PSNR} 的值随着强度因子增大而降低,当 $\beta < 0.2$ 时,难以提取的完整的水印;当 $\beta > 0.8$ 时,载体图像嵌入水印后其视觉质量较差。因此,在实际使用中应该选择一个较合理的水印强度因子,使其既能较好地嵌入水印信息,又能有较好的载体图像质量。为了获得最佳强度因子,定义评价函数为 $f_{\text{Eva}}(\beta) = |h' - h_0|^2 + |\omega' - \omega_0|^2$ 。进行了优化计算求评价函数的最小值,得最佳 β 约为 0.35。

表 1 强度因子 β 和 f_{PSNR} 的关系

Table 1 Intensity factor versus PSNR

| β | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 |
|-------------------|------|------|------|------|------|------|------|
| f_{PSNR} | 47.6 | 46.1 | 43.5 | 41.8 | 40.1 | 39.7 | 38.3 |

4 水印的嵌入、提取和稳健性测试

实验采用标准测试图 cameraman 作为载体图像。水印信息分别采用二值图像和 256 灰阶 Lena 图像。所有图像都是分辨率都是 256 pixel \times 256 pixel。级联分数傅里叶变换系统参数同上面的收敛性实验,迭代次数选为 10。图 4 给出了二值水印和灰阶水印的嵌入实验结果。(a)为嵌入二值水印的载体图像,(b)为提取的二值水印;(c)为嵌入灰阶水印的载体图像,(d)为提取的灰阶水印。实验中,从视觉不可见性、抗噪声的稳健性和抗图像处理的稳健性这三个方面对算法进行了检测。抗图像处理的稳健性主要从剪切、旋转和中值滤波等方面考查。本算法利用两个相位分布函数作为密钥保护嵌入的水印信息,无密钥或使用错误密钥都无法提取水印。

4.2 抗噪声叠加稳健性测试

图 5(a),(d)和(g)分别为添加了高斯噪声、椒盐噪声和乘性噪声(方差均为 0.05)的载体图像,从中仍然可以提取出相应的二值水印[分别为图 5(b),(e)和(h)]和灰阶水印[分别为图 5(c),(f)和(i)],可见水印提取的效果非常好,与添加噪声前提取的水印差别很小。图 6(a),(b)给出了载体图像和二值水印的 f_{NMSE} 随加入三种噪声方差的变化曲线。随着噪声方差的增加,载体图像的 f_{NMSE} 逐渐增加,增长趋势因噪声类型而不同;提取水印的 f_{NMSE} 也随着噪声方差而增加,而且 f_{NMSE} 增长趋势基本与噪声类型无关,当噪声方差达到约 0.05 以后,水印的 f_{NMSE} 基本平稳振荡。实验说明该算法有极强的抗噪声的稳健性。

4.3 抗图像处理稳健性测试

一般图像处理操作会移除载体图像的部分信息,从中提取的水印信息不可避免的受到影响。在这种情况下,能正确地检测到水印的存在是非常重要的。如图 7 所示,在剪切掉 30% 的像素、旋转

20°、中值滤波和缩放 75% 的处理下,用本文提出的水印算法,仍能够检测并提取水印。表 2 给出从各种图像处理攻击后的载体图像提取的二值及灰阶水

印的归一化均方差。可以看出,仍可检测并提取水印信息,实验说明此算法具有较好的抗图像处理稳健性。



图 5 抗噪声稳健性实验结果. (a) 叠加高斯噪声的载体图像; (b) 提取的二值水印; (c) 提取的灰阶水印; (d) 叠加椒盐噪声的载体图像; (e) 提取的二值水印; (f) 提取的灰阶水印; (g) 添加乘性噪声的载体图像; (h) 提取的二值水印; (i) 提取的灰阶水印

Fig. 5 Robustness experiments against noise addition. (a) host image with gauss noise; (b) extracted binary watermark; (c) extracted gray-level watermark; (d) host image with pepper noise; (e) extracted binary watermark; (f) extracted gray-level watermark; (g) host image with multiplicative noise; (h) extracted binary watermark; (i) extracted gray-level watermark

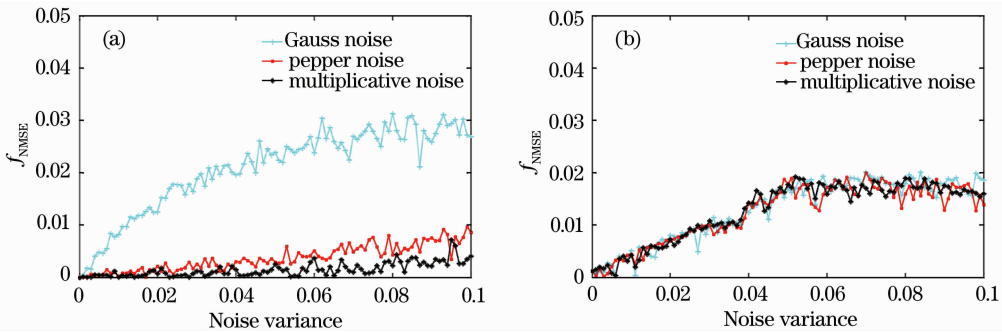


图 6 归一化均方差随噪声方差曲线. (a) 载体图像的 f_{NMSE} 随噪声方差曲线; (b) 二值水印的 f_{NMSE} 随噪声方差曲线

Fig. 6 f_{NMSE} versus noise variance. (a) f_{NMSE} of host images versus noise variance; (b) f_{NMSE} of binary watermarks versus noise variance



图 7 抗图像处理稳健性实验. (a) 剪切 30%; (b) 旋转 20°; (c) 中值滤波; (d) 缩放 75%

Fig. 7 Robustness experiments against image processing. (a) shearing; (b) rotation; (c) medium filtering; (d) resizing

表 2 载体图像攻击后提取水印的归一化均方差

Table 2 f_{NMSE} of extracted watermark from attacked host images

| Watermark type | shearing | rotation | filtering | resizing |
|----------------|----------|----------|-----------|----------|
| binary | 0.0637 | 0.1189 | 0.1033 | 0.1135 |
| gray-level | 0.1532 | 0.2014 | 0.1931 | 0.2042 |

4.4 数字水印算法安全性分析

此算法利用迭代分数傅里叶变换将水印信息嵌入到载体图像中,并得到输入域和中间域的相位分布作为密钥,实现了一种加密水印算法。图 8 为安全性实验结果,图 8(a)为无相位密钥 key_1 的情况下从嵌入水印的载体图像中提取的水印,可以看出提取的信息杂乱无章,与原水印信息无关;图 8(b)为无相位密钥 key_2 的情况下从嵌入水印的载体图像中提取的水



图 8 安全性分析实验结果。(a)无相位密钥 key_1 情况下提取的水印;(b)无相位密钥 key_2 情况下提取的水印;(c)使用错误相位密钥 key_2 提取的水印

Fig. 8 Security analysis of this watermarking method. (a)extracted watermark without phase key1;(b)extracted watermark without phase key2;(c)extracted watermark with wrong phase key2

5 结 论

本文基于光学级联分数傅里叶变换系统,提出一种利用迭代分数傅里叶变换和随机相位编码的加密数字水印技术。该技术利用两个相位分布函数作为相位密钥保护水印,无密钥时无法提取水印,具有极高的安全性。实验结果验证该算法嵌入的图像水印具有视觉不可见性,并且对常见的图像处理攻击和噪声干扰具有很好的稳健性。该数字水印技术基于光学分数傅里叶变换原理,利用数字变换或光学变换都能方便的实现,可作为一种信息隐藏及保护的有效方案。

参 考 文 献

- Sun Shenghe, Lu Zheming, Niu Xiamu. Digital watermarking technique and application [M]. Beijing: Science Press, 2004, 32~36
孙圣和,陆哲明,牛夏牧. 数字水印技术及应用 [M]. 北京: 科学出版社, 2004, 32~36
- Peng Xiang, Wei Hengzheng, Zhang Peng. Introduction to optical information security [M]. Beijing: Science Press, 2008, 1~11

印的,该图像为翻转的载体图像,也不含原水印信息;图 8(c)为使用错误相位密钥 key_2 从嵌入水印的载体图像中提取的水印,该图为伪随机噪声分布也不含原水印信息。该算法的安全性极高,主要由于(1)密钥为二维相位分布,密钥空间极大,如本实验中选取 $256 \text{ pixel} \times 256 \text{ pixel}$,每个像素为 $0 \sim 2\pi$ 内的 256 阶随机相位,密钥空间在 10 的十五万次幂以上。(2)相位密钥对于空间位置极其敏感,当其横向位置偏离 $1/10$ 像素距离以上,就无法正确提取水印,故相位密钥的空间坐标也可作为系统密钥进一步增加系统的安全性。(3)相位密钥具备将输入域图像散布到输出域的性质,使得输出域上每一像素都包含输入域的所有像素的信息,因此该水印算法对噪声和几何变形攻击表现出了很好的稳健性。

彭 翔,位恒政,张 鹏. 光学信息安全导论[M]. 北京: 科学出版社, 2008, 1~11

- Peng Xiang, Zhang Peng, Niu hanben. 3D spatial digital watermarking system based on virtual optics[J]. *Acta Optica Sinica*, 2004, **24**(11): 1507~1510
彭 翔,张 鹏,牛憨笨. 基于虚拟光学的三维空间数字水印系统[J]. 光学学报, 2004, **24**(11): 1507~1510
- Yuchi Liang, Gu Jihua, Liu Wei *et al.*. An image digital watermark technique based on digital holography and discrete cosine transform [J]. *Acta Optica Sinica*, 2006, **26** (3): 355~361
尉迟亮,顾济华,刘 薇等. 基于数字全息及离散余弦变换的图像数字水印技术[J]. 光学学报, 2006, **26**(3): 355~361
- Liu Zhengjun, Zhao Haifa, Zhu Banghe *et al.*. Fractional Fourier Domain Digital Watermarking[J]. *Acta Photonica Sinica*, 2003, **32**(3): 332~335
刘正君,赵海发,朱邦和等. 分数傅里叶域数字水印算法[J]. 光子学报, 2003, **32**(3): 332~335
- Peng Xiang, Bai Weidong, Tian Jindong. Digital watermarking with half-tone encoded computer-generated hologram[J]. *Acta Optica Sinica*, 2007, **27**(6): 1011~1017
彭 翔,白伟东,田劲东. 半色调编码计算全息图的数字水印方法[J]. 光学学报, 2007, **27**(6): 1011~1017
- Sun Liujie, Zhuang Songlin. Anti-fake technique by double random phase encrypted holographic mark [J]. *Acta Optica Sinica*, 2007, **27**(1): 31~34
孙刘杰,庄松林. 双随机相位加密全息标识防伪技术研究[J]. 光学学报, 2007, **27**(1): 31~34

- 8 Sun Liujie, Zhuang Songlin. Identification mark of encrypted in-line fresnel holography[J]. *Chinese J. Lasers*, 2007, **34**(3): 402~405
孙刘杰, 庄松林. 基于同轴菲涅耳全息标识印刷防伪技术[J]. *中国激光*, 2007, **34**(3): 402~405
- 9 Shannon C E. Communication theory of secrecy system[J]. *Bell. Syst. Tech.*, 1949, **28**: 656~715
- 10 Hans Delfs, Helmut Knebl. Introduction to cryptography[M]. Springer, 2007, 1~6
- 11 Yang Bo. Modern Cryptography [M]. Beijing: Tsinghua Univ. Press, 2007. 1~11
杨波. 现代密码学 [M]. 北京: 清华大学出版社, 2007. 1~11
- 12 Ji Jin, Huang Fei, Wang Liang *et al.*. Information encryption based on digital holography and phase retrieve algorithm[J]. *Chinese J. Lasers*, 2007, **34**(10): 1408~1412
季瑾, 黄飞, 王亮等. 利用数字全息和相位恢复算法实现信息加密[J]. *中国激光*, 2007, **34**(10): 1408~1412
- 13 Bahram Javidi. Optical and digital techniques for information security[M]. Springer, 2005, 113~134
- 14 Namias V. The fractional order Fourier transform and its application to quantum mechanics[J]. *IMA J. Appl. Maths.*, 1980, **25**(1): 241~265
- 15 Mendlovic D, Ozaktas H. M. Fractional fourier transforms and their optical implementation[J]. *J. Opt. Soc. Am. A*, 1993, **10**: 1875~1881
- 16 Aysegul Sahin, Haldun M. Ozaktas, David Mendlovic. Optical implementations of two-dimensional fractional Fourier transforms and linear canonical transforms with arbitrary parameters[J]. *Appl. Opt.*, 1998, **37**(11): 2130~2141
- 17 A. W. Lohmann. Image rotation, Wigner rotation, and fractional Fourier transform[J]. *J. Opt. Soc. Am. A*, 1993, **10**(10): 2181~2186
- 18 G. Unnikrishnan, J. Joseph, K. Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. *Opt. Lett.*, 2000, **25**(12): 887~889