第 31 卷第 2 期　　四川理工学院学报(自然科学版)　　Vol. 31　No. 2
2018 年 4 月　　Journal of Sichuan University of Science & Engineering(Natural Science Edition)　　Apr. 2018
文章编号:1673-1549(2018)02-0075-08　　DOI:10.11863/j.suse.2018.02.12

一种基于干涉的新型图像加密算法

马文林[1,2], 张　刚[2], 韩　超[1]

(1.安徽工程大学电气工程学院, 安徽　芜湖　241000; 2.皖西学院电气与光电工程学院, 安徽　六安　237012)

摘　要:针对干涉加密方案中图像解密时存在的轮廓问题,提出了一种小波数字水印和混沌序列相结合的分数傅里叶干涉图像加密方法。首先通过分数傅里叶干涉将明文信息编码到两个相位掩模中,进行初次加密;然后利用小波数字水印理论,将相位掩模作为水印,嵌入到宿主图像中进行再次加密;最后对加密后的宿主图像利用混沌序列实行像素值替换操作完成整个加密过程。该加密方法能够将编码所得的两个相位掩模隐藏起来,非法解密者无法通过利用一块或者两块相位掩模来获得原始图像的轮廓信息,整个加密过程设计简单、秘钥具有良好的敏感性,且后两次加密具有随机性,从而提升了整个加密系统的鲁棒性。仿真结果表明,该方法具有良好的可行性,且解密恢复出的图像质量理想、安全性高。

关键词:干涉;图像加密;数字水印;混沌映射;分数傅里叶

中图分类号:O438　　**文献标志码**:A

引　言

近几十年以来,随着信息技术的高速发展,信息安全成为研究的热点问题,光学图像加密技术因其高速并行处理的能力,受到了越来越多的关注[1-3]。1995 年,Refregier 和 Javidi 提出了一种使用双随机相位掩模将原始图像编码为平稳白噪声[4]的加密方法。研究者将该方案中提出的随机相位编码(Random Phase Encoding, RPE)方法广泛地应用到光学图像加密系统当中[5-8]。实验表明,仅用双随机相位编码(Double Random Phase Encoding,DRPE)加密的方案在抵抗攻击方面存在缺陷[9-10]。为了进一步提高图像加密系统的安全性,研究人员在 DRPE 基础上提出了一系列新的加密方法,如迭代相位检索方法[11-13]、混沌置乱加密方法[14-17]等。Zhang 等[18]最早提出了一种基于干涉的光学图像加密方法,该加密方法提出对原始图像波函数进行分解,可以获得两个相位掩模,其中,一个作为明文,另一个作为密文。解密时通过利用相干光束调制,即可在输出平面直接获得原始图像,该加密过程简洁明了,解密光路设置简单。Chen 等[19]利用相同的思路提出了一种基于

收稿日期:2017-12-26

基金项目:安徽省教育厅高校自然科学研究项目(KJ2016A056);安徽省自然科学基金面上项目(1508085MF121、1408085MA20);安徽省级重点实验室开放课题(1506c085002);安徽省教育厅人才项目(gxfxZD2016100、gxyqZD2016242)

作者简介:马文林(1994-),男,安徽淮北人,硕士生,主要从事光学加密与图像处理方面的研究,(E-mail)798621744@qq.com;
张　刚(1975-),男,安徽六安人,教授,博士,主要从事自动控制等方面的研究,(E-mail)zhanggang@wxc.edu.cn

通信作者:韩　超(1974-),男,安徽宿州人,副教授,博士,主要从事光信息处理、图像处理、全息显示等方面的研究,(E-mail)hanchaozh@126.com

Arnold 变换和干涉的彩色图像加密方法,彩色图像被分解成三个独立的通道,结合 Arnold 变换和干涉方法将每个通道加密成两个随机相位掩模。然而干涉加密方式存在着严重的缺陷,即非法解密者通过利用分析获得的两块相位掩膜的任一块,即可获得原始图像的轮廓信息。在 Chen 提出的加密方案中,只单纯地将干涉方法应用到彩色图像当中,并没有解决干涉加密方式中出现的轮廓问题。

为了解决干涉加密过程中出现的轮廓问题,研究者们提出了不同的解决方案。Zhang 等[20]提出了一种基于交换两个掩模中位置相同部分的保密增强方案,即在获得两块掩模后,随机选择第一块掩模的部分,进而将其与第二块掩模相同位置的部分进行交换,每次随机选择掩模相同的位置和像素块的大小,这种方法需要耗时选定图像的大小和位置进行交换,若进行交换的次数有限,非法解密者还是能够获得原始图像的信息。Wang 等[21]提出了一种光学图像隐藏与干涉轮廓消除的方案,通过引入一个随机位相函数,结合对图像分析获得的两块相位掩模,可以将原始图像傅里叶频谱隐藏到三个相位掩模当中,这种方法可以解决基于干涉加密方案中两个相位掩模出现的轮廓问题,但是增加了解密过程的复杂度,如果潜在的攻击者同时获取三个相位掩模中的两个,那么将会消除引入的相位掩模的随机调制,在验证过程中仍然可以检测到轮廓图像。Wang[22]提出了一种基于干涉和相位混合处理的光学图像加密与轮廓隐藏的方案,提出将原始图像的信息隐藏在三个相位掩模当中的新方法,其中一个掩模是随机相位函数,另两个掩模通过分析获得,通过引入线性相位混合运算理论,利用正交矩阵对获得的三个相位掩模进行变换,增强了加密的安全级别,不足之处在于,当处理大量的像素数据时,利用这种方法会增加实验的复杂度,整个加密过程的效率还有待提高。Zhong 等[23]提出一种多参数分数阶傅里叶域的无轮廓干涉加密的方案,首先对待加密图像进行混沌像素置乱(Chaotic Pixel Scrambling,CPS),然后编码成复信号的实部,复信号在离散多参数分数阶傅里叶变换域中产生三个相位掩模,将原始的图像信息隐藏在三个相位掩模当中,此加密方法安全性较高,但是在解密时需要叠加三个相位掩模以及进行多参数分数傅里叶变换的解密,虽具有较强的抗干扰性,但是利用混沌像素置乱和多参数分数傅里叶变换方法生成了过多的秘钥数量,增加了加密过程的计算量。Kumar 等[24]提出使用拼图变换(Jigsaw Transformation,JT)算法进行基于干涉的图像加密方案,原始图像通过分块置乱,转换成随机图案,将获得的相位掩模划分成多个块,并根据置换矩阵对其位置进行置乱,在此方法中,JT 被应用于解决轮廓问题,提高加密方法的安全性,在其解密过程中,通过使用单个空间光调制器(SLM)来显示两个相位掩模的叠加,然而,在解密之前恢复相位掩模需要进行逆计算,大量的数据计算降低了整个系统的加密效率。

在本文中,针对干涉图像加密出现的轮廓问题提出了一种新的解决方案,将原始图像进行计算分析后获得两块相位掩模,利用小波数字水印理论,将两块相位掩模作为水印嵌入到宿主图像中,对宿主图像利用混沌序列与像素值的替换操作实现混沌加密,可灵活设定密钥位数,秘钥具有良好的敏感性。待加密图像经过三次加密后,所获得的密文具有良好的鲁棒性和不可见性,而且整个加密和解密过程没有复杂的计算,从而提升了整个加密系统的加密解密效率,解密过程可以使用数字结合光路实现,具有良好的解密恢复效果,避免了干涉加密中出现的轮廓问题。

1 干涉图像加密

基于光学干涉加密是将图像编码成两个相位掩模[18],此方法的编码过程简单,通过计算分析获得两个相位掩模。本文采用分数傅里叶方法获得两个相位掩模,同时在加密过程中使用的分数傅里叶阶数可以作为秘钥来使用。将两个掩模 $M1$ 和 $M2$ 分配给两个不同的重要人员,只有当两个掩模正确时,才能通过数字或者光路实现正确解密。对于被加密的图像 $I(m,n)$,可以构造一个新的对象函数:

$$I'(m,n) = \sqrt{I(m,n)}R(m,n) \tag{1}$$

其中:$R(m,n) = \exp(i2\pi rand(m,n))$,$rand(m,n)$ 表

示 $m \times n$ 维,取值范围为(0,1)的随机分布矩阵。为了进一步提升系统的安全性能,可以将 $R(m,n)$ 通过两个随机相位函数 $R_1(m,n)$ 和 $R_2(m,n)$ 的干涉来表示,其中:

$$R_1(m,n) = \exp(iM1)$$

$$R_2(m,n) = \exp(iM2)$$

则有:

$$I'(m,n) = FrFT^{(\alpha,\beta)}[R_1(m,n)] + FrFT^{(\alpha,\beta)}[R_2(m,n)] \quad (2)$$

其中,$FrFT$ 表示分数傅里叶变换(Fractional fourier transform,FrFT),α 和 β 表示分数傅里叶的阶数[23]。经过推导得到:

$$R_2(m,n) = FrFT^{-1(\alpha,\beta)}[I'(m,n)] - R_1(m,n) \quad (3)$$

根据相位函数的性质可得:

$$[FrFT^{-1(\alpha,\beta)}[I'(m,n)] - R_1(m,n)] \times [FrFT^{-1(\alpha,\beta)}[I'(m,n)] - R_1(m,n)]^* = 1 \quad (4)$$

其中,$*$ 代表函数的共轭。两块相位掩模板的函数表达式:

$$M1 = \arg\{FrFT^{-1(\alpha,\beta)}[I'(m,n)]\} - \arccos\{\mathrm{abs}(FrFT^{-1(\alpha,\beta)}[I'(m,n)])/2\} \quad (5)$$

$$M2 = \arg\{FrFT^{-1(\alpha,\beta)}[I'(m,n)] - R_1(m,n)\} \quad (6)$$

2　数字水印图像加密

本文中所使用的水印加密算法是基于 Haar 小波变换的水印加密方法[25-28],首先对水印图像进行具有纠错能力的二进制编码(BCH 编码),将其编码成二进制序列。通过对原始明文信息进行处理,来选择固定的小波系数,从图像的鲁棒性和隐藏性的折中考虑,在嵌入水印序列时选择中频系数来嵌入水印序列。把选择的小波中频系数进行等大小块的划分,将所有块内系数幅值的累积和与单个系数块大小做除法运算,即可得到每个系数块的平均值,其中块的大小和嵌入水印比特的量成反比。水印序列的嵌入实质上是对系数块的平均值进行量化完成的,在量化过程中,对小波系数从 $N,N-1,\cdots,1$(N 为整数)层次做间隔逐渐减小的量化,将系数平均值量化到与之最近的整数奇偶点,最终完成二进制水印序列的嵌入。在此过程中,水印嵌入所使用 BCH 编码可作为秘钥使用,同时利用到的 Haar 小波基、选择小波中频系数区域、小波分解的层数均可作为密码使用,从而提高了信息传输的安全性。

3　混沌映射图像加密

采用 Logistic 混沌映射模型生成对应混沌序列,利用混沌序列对图像像素值的位置进行置乱操作,从而实现对图像加密[29]。

Logistic 混沌映射是一维非线性映射,它的模型如下:

$$x_{n+1} = \mu x_n(1 - x_n) \quad (7)$$

其中:$0 < \mu \leqslant 4$,$0 < x < 1$,$n \in \mathbf{N}$;$x_n \in [0,1]$,μ 为分岔参数。当 $3.56994\ldots < \mu \leqslant 4$ 时,映射进入混沌区域。

利用上述混沌映射模型,假设图像 $O(i,j)$ 处的灰度值为 $X(i,j)$,在相同位置进行替换后的灰度值表示为 $X'(i,j)$,像素值的替代是在空域中进行的,替换过程为:

$$X'(i,j) = \{\{r_1(i,j) \oplus X(i,j) \oplus r_2(i,j) + L - r_3(i,j)\} \bmod L\} \bmod 256 \quad (8)$$

其中:L 表示图像的颜色深度;mod 表示求模运算;$\oplus$ 表示按位异或运算;r_1、r_2、r_3 表示利用混沌系统最终得到的混沌序列值,分别对应的混沌映射初始值 x_1、x_2、x_3 和分岔参数 μ_1、μ_2、μ_3,作为秘钥使用。

4　图像加密方案

整体加密方案示意图如图 1 所示。首先对原始 Lena图像进行分数傅里叶编码,可获得两个相位掩模 $M1$ 和 $M2$,这里选择 $M1$ 作为明文、$M2$ 作为密文,同时分数傅里叶的阶数也作为秘钥,从而完成初次加密;将获得的相位掩膜 $M1$ 作为水印图像,利用基于 Haar 小波变换的水印加密方法将 $M1$ 嵌入到宿主图像 Host image1 当中,嵌入水印后的图像为 Embedded image1,即 $A1$。使用同样的方法将 $M2$ 作为水印嵌入 Host image2 中,嵌入水印后的图像为 Embedded image2,即 $A2$,其中使用的

BCH 编码、利用到的 Haar 小波基、选择小波中频系数区域、小波一层分解的层数作为加密秘钥,从而完成了再次加密;利用混沌序列像素值替换方法,对 *A*1 和 *A*2 分别进行混沌映射图像加密,得到最终的加密图像 *B*1 和 *B*2,其中由用户设定的多位混沌映射参数作为加密秘钥,从而完成整个加密过程。

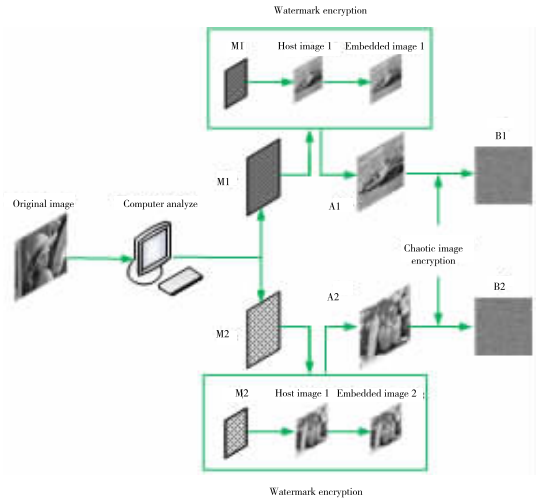


图 1 加密方案示意图

5 图像解密方案

整体解密方案光路图如图 2 所示,其中,Laser 为激光源、BCE 为光束准直器和扩束器、SLM 为空间光调制器、Lens 为透镜。在计算机中完成对混沌映射的解密和水印的提取,从而解密出 *M*1 和 *M*2,结合相应的光学系统将 *M*1 和 *M*2 重构出原始 Lena 图像。

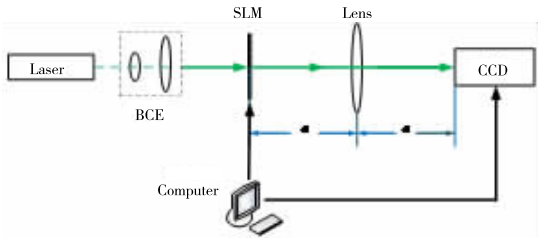


图 2 解密方案示意图

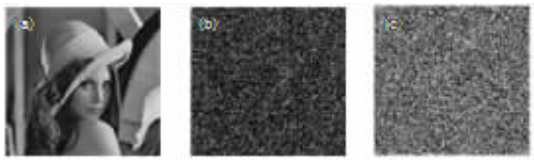
在解密时,首先进行混沌映射解密,它是混沌映射加密过程的逆过程,由用户设定的多位混沌映射参数作为解密秘钥。解密过程为:

$$X(i,j) = \{r_1(i,j) \oplus \{[X'(i,j) + r_3(i,j)] \bmod L\} \oplus r_2(i,j)\} \bmod 256 \quad (9)$$

通过混沌图像解密后,对解密图像进行数字水印提取,检测图像中的水印信息,根据密钥确定嵌入水印的位置,完成水印的提取,其中使用 BCH 编码、利用到的 Haar 小波基、选择小波中频系数区域、小波一层分解层数作为解密秘钥。在计算机中经过上述两次解密,即可获得两个相位掩膜 *M*1 和 *M*2,两个相位掩膜通过计算机控制,将 *M*1 和 *M*2 叠加输入到 SLM 中,经过激光调制后,通过透镜实现分数傅里叶的逆运算,即可在 CCD 上获得解密的 Lena 图像,完成整个解密过程。其中 $d = [1 - \cos(\frac{a\pi}{2})]f$, a 为分数傅里叶的阶数,f 为透镜的焦距[30]。

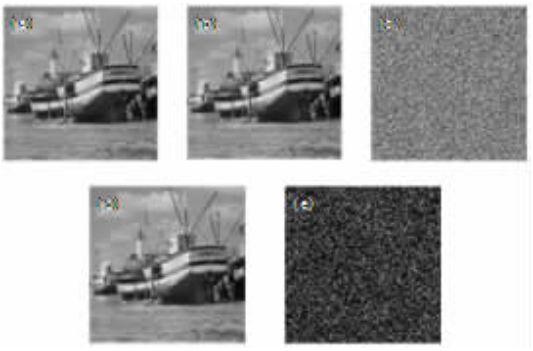
6 仿真与分析

首先在理论分析的基础上,利用计算机进行仿真,将像素数为 256 ×256、灰度级为 256 的原始 Lena 图像,通过分数傅里叶干涉图像加密,编码得到两个相位掩膜 *M*1 和 *M*2,分别作为明文和密文。由于所使用 Lena 图像行列数相同,同时在光路解密中使二维分数傅里叶阶数通过一块透镜实现解密,所以要保证图像沿 x 和 y 轴方向变化阶数相同,这里阶数取 $\alpha = \beta = 0.5$,仿真结果如图 3 所示。将 *M*1 和 *M*2 作为水印,利用基于 haar 小波的数字水印加密方法,将 *M*1 嵌入到宿主图像 Boat 当中的中频区域,选择的小波分解层数为一层,嵌入水印后的图像如图 4(b)所示,利用同样的方法将 *M*2 嵌入到宿主图像 Pepper 当中,嵌入水印后的图像如图 5(b)所示,通过仿真结果表明,嵌入水印后的图像和原宿主图像之间的相关系数良好,具体数值见表 1。利用混沌序列像素值替换方法对嵌入水印后的载体图像进行混沌映射加密,混沌映射加密和解密的秘钥由操作者设定的 6 位秘钥来控制,前三位为初始值,后三位分别对应着前三位的混沌变换的分岔参数,通过混沌变换即可得到三位混沌序列值,这里设定的秘钥为[0.331 0.433 0.63 3.756 3.92 3.85],最终得到的加密图像如图 4(c)和图 5(c)所示。宿主图像作为载体图像可以任意选择,为了区别原始明文图像,这里所选的宿主图像为 Boat 和 Pepper 图像。



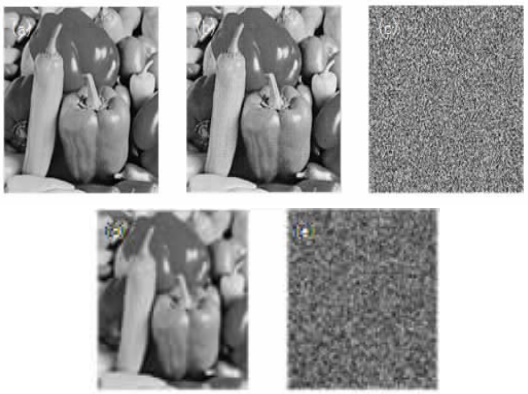
(a)原始图像　(b)相位掩膜$M1$　(c)相位掩膜$M2$

图 3　Lena 图像编码



(a)宿主图像;(b)水印$M1$嵌入后的图像;(c)混沌映射加密后的图像;(d)混沌映射解密后的图像;(e)重构的$M1$图像

图 4　图像 Boat 处理过程



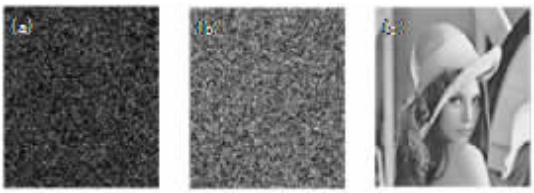
(a)宿主图像;(b)水印$M2$嵌入后的图;(c)混沌映射加密后的图像;(d)混沌映射解密后的图像;(e)重构的$M2$图像

图 5　图像 Pepper 处理过程

表 1　归一化相关系数

图　像	嵌入水印 M1 后的宿主图像,图 4(b)	嵌入水印 M2 后的宿主图像,图 5(b)	混沌解密前图像,图 7(a)	原始明文图像,图 3(a)
	嵌入水印 M1 前的宿主图像,图 4(a)	嵌入水印 M2 前的宿主图像,图 5(a)	混沌解密后图像,图 7(d)	最终重构图像,图 6(c)
归一化相关系数(NC)	0.9904	0.9862	1	0.9854

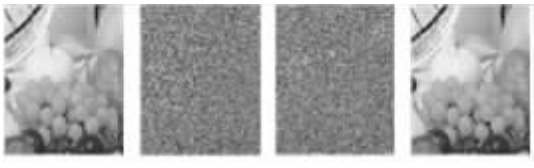
整体解密的过程为加密过程的逆过程,首先对混沌映射加密后的图像进行像素值替换解密操作,得到混沌映射解密图像,解密秘钥同加密秘钥相同,混沌映射解密出的图像如图 4(d)和图 5(d)所示;分别对两幅混沌映射解密图像进行小波数字水印的逆变换,进行水印的提取,解密秘钥同加密秘钥相同,即可提取出水印图像 *M1* 和 *M2*,如图 4(e)和图 5(e)所示。利用解密得到的 *M1* 和 *M2*,通过分数傅里叶干涉的逆编码操作,即可重构出原始 Lena 图像,如图 6(c)所示。



(a)重构的$M1$图像　(b)重构的$M2$图像　(c)最终重构的图像

图 6　Lena 图像重构

为了对本文中混沌加密算法进行性能分析,单独对其秘钥进行敏感性测试,采用正确秘钥以及与之差异微小的另一组秘钥分别对密文图像进行解密实验,实验选取图像可以任意选择,这里选择像素大小为 256 × 256 的 Fruits 图像,由于所使用的秘钥中第一位到第三位参数与第四位到第六位参数对应着三组 Logistic 映射的初始值 x_0 和分岔参数 μ,通过改变其中一组来查看仿真结果。正确解密时 $x_0 = 0.331$, $\mu = 3.756$。图 7(b)中参数设置为 $x_0 = 0.331001$、$\mu = 3.756$;图 7(c)中参数设置为 $x_0 = 0.331$、$\mu = 3.756001$。由图 7(b)和图 7(c)中可以看出秘钥位数相差 10^{-6} 就得到一副完全显示不出任何明文信息的错误解密图像。在秘钥正确时,混沌映射解密的图像如图 7(d)所示。



(a)　(b)　(c)　(d)

图 7　秘钥安全性分析

为了进一步验证混沌映射加密算法的秘钥灵敏程度,采用均方误差(MSE)来衡量原始 Fruits 图像和

不同秘钥解密后图像的相似程度。从图 7 分析可得,解密秘钥参数一旦发生细微偏差,重构出的图像即为噪声图像。设置混沌映射初始参数的偏差,观察偏差对解密图像与原始图像的 MSE 值的影响,其中 $a = x_0 = 0.331$, n 为指数,从图 8 显示的密钥敏感性分析可知,当秘钥偏差精确到小数点 16 位以后,对 MSE 的值不产生影响,说明此加密方法所采用的秘钥具有良好的敏感性,微小的秘钥偏差会重构出错误的图像。均方误差的定义为:

$$MSE(h_1,h_2) = \frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N} |h_2(i,j) - h_1(i,j)|^2 \tag{10}$$

其中:$N \times N$ 为图像的大小,$h_1(x,y)$ 和 $h_2(x,y)$ 分别代表原图和解密图像的灰度值。

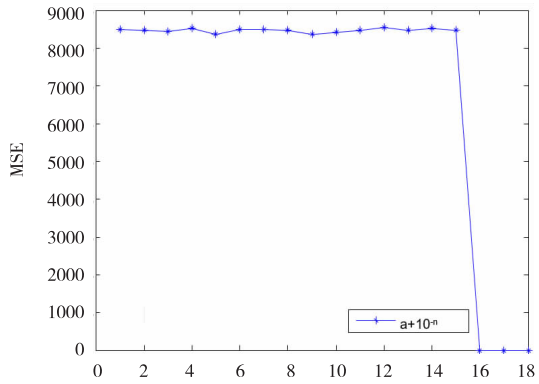


图 8 秘钥敏感性分析

在本文加密方案中,整体解密图像的质量可以通过归一化相关系数(NC)进行定量评估,这可以反映解密图像和加密图像的相关性,表示为:

$$NC = \frac{\sum_{i=1}^{K}\sum_{j=1}^{L} R(i,j) \cdot O(i,j)}{\sum_{i=1}^{K}\sum_{j=1}^{L} O^2(i,j)} \tag{11}$$

其中:R 表示解密图像,O 表示加密图像,(i,j) 分别表示图像上的像素,K、L 分别表示图像的行数和列数。通过仿真表明,嵌入水印后的图像与原始图像的相关系数优良,通过混沌解密能够很好重构出混沌加密前的图像,最终重构出的 Lena 图像保持着良好的图像质量(表 1)。

7 结束语

在运用了数字水印理论和混沌图像加密的方法的基础上,提出一种新的干涉数字水印加密方法,该方法对图像进行相位的编码、数字水印的嵌入和混沌像素值替换三种操作,完成对图像的安全加密,从而避免了重构时出现的轮廓问题,从仿真结果来看,本文中所使用的加密方案不仅确保了图像的安全传输问题,并且能很好地重构出原始图像,并且在加密的过程中能够抵抗一定的噪声干扰,这使得整体的鲁棒性得到提升的同时,整体的加密安全性也得到提高。

参 考 文 献:

[1] ALFALOU A,BROSSEAU C.Optical image compression and encryption methods[J].Advances in Optics & Photonics,2009,1(3):589-636.

[2] JAVIDI B.Optical and digital techniques for information security[J].Proceedings of the IEEE,2009,97(6):1128-1148.

[3] CHEN W,JAVIDI B,CHEN X.Advances in optical security systems[J].Advance in Optics & Photonics,2014,6(6):120-155.

[4] REFREGIER P,JAVIDI B.Optical image encryption based on input plane and Fourier plane random encoding[J].Optics Letters,1995,20(7):767-769.

[5] ZHU B,LIU S,RAN Q.Optical image encryption based on multifractional Fourier transforms[J].Optics Letters,2000,25(16):1159-1161.

[6] CHEN J X,ZHU Z L,LIU Z,et al.A novel double-image encryption scheme Based on cross-image pixel scrambling in gyrator domains[J].Opt Express,2014,22(6):7349-7361.

[7] SITU G,ZHANG J.Double random-phase encoding in the Fresnel domain[J].Optics Letters,2004,29(14):1584-1586.

[8] SUI L,DUAN K,LIANG J.Double-image encryption based on discrete multiple parameter fractional angular transform and two-coupled logistic maps[J].Opt Communications,2015,

343:140-149.

[9] PENG X, ZHANG P, WEI H, et al. Known-plaintext attack on optical encryption based on double random phase keys[J].Optics Letters,2006,31(8):1044-1046.

[10] FRAUEL Y, CASTRO A, NAUGHTON T J, et al. Resistance of the double random phase encryption against various attacks[J].Optics Express,2007,15(16): 10253-10265.

[11] LIU Z,GUO Q,XU L,et al.Double image encryption by using iterative random binary encoding in gyrator domains[J].Optics Express,2010,18(11):12033-12043.

[12] SITU G,ZHANG J.A lensless optical security system based on computer generated phase only masks[J]. Optics Communications,2004,232:115-122.

[13] WANG H E,CHANG H,LIE W.Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems [J].Optics Express,2009,17(16):13700-13710.

[14] HENNELLY B,SHERIDAN J T.Optical image encryption by random shifting in fractional Fourier domains [J].Optics Letters,2003,28(4):269-271.

[15] LIU Z,LI Q,DAI J.Image encryption based on random scrambling of the amplitude and phase in the frequency domain[J]. Optical Engineering,2009,48(8): 771-777.

[16] LU D J,HE W Q,LIAO M H,et al.Discussion and a new method of optical cryptosystem based on interference[J]. Opt Laser Eng,2017,8(9):13-21.

[17] GONG Q,WANG Z P,LV X D,et al. Interference-based image encryption with silhouette removal by aid of compressive sensing[J]. Optics Communications, 2016,359:290-296.

[18] ZHANG Y,WANG B.Optical image encryption based on interference[J]. Optics Letters,2008,33(21): 2443-2445.

[19] CHEN W,QUAN C.Optical color image encryption based on Arnold transform and interference method [J].Optics Communications,2009,282:3680-3685.

[20] ZHANG Y,WANG B.Enhancement of image hiding by exchanging two phase masks[J].Journal of Optics A Pure & Applied Optics,2009,11(12):1254061-1254064.

[21] WANG X,ZHAO D.Optical image hiding with silhouette removal based on the optical interference principle[J].Applied Optics,2012,51(6):686-691.

[22] WANG Q. Optical image encryption with silhouette removal based on interference and phase blend processing[J]. Optical Communications, 2012, 285: 4294-4301.

[23] ZHONG Z,QIN H,LIU L,et al.Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain[J]. Optics Express,2017,42(6):6974-6982.

[24] KUMAR P,JOSEPH J,SINGH K.Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light Modulator[J].Applied Optics,2011,50(13): 1805-1811.

[25] 于润伟,朱晓慧.基于 Haar 小波变换的数字图像水印算法[J].黑龙江大学工程学报,2006,33(1):127-129.

[26] 肖亮,吴慧中,韦志辉.基于整数小波变换的图像鉴定数字水印技术[J].计算机工程与应用,2001,37(8):21-23.

[27] 杨垚婷.基于小波变换的数字水印算法的研究与实现[D].成都:成都理工大学,2017.

[28] 牛夏牧,陆哲明,孙圣和.基于多分辨率分解的数字水印技术[J].电子学报,2008,28(8):1-4.

[29] 柳娜.基于混沌的数字图像加密算法的研究[D].哈

尔滨:哈尔滨理工大学,2012.

[30] 文亮.分数傅里叶变换及其应用[D].重庆:重庆大学,2008.

A Novel Image Encryption Algorithm Based on Interference

MA Wenlin[1,2], *ZHANG Gang*[2], *HAN Chao*[1]

(1. School of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China; 2. School of Electrical and Photoelectronic Engineering, West Anhui University, Lu'an 237012, China)

Abstract: Based on the silhouette problem existing in the image decryption of the interference encryption scheme, a fractional Fourier interference image encryption scheme combining wavelet digital watermark and chaotic sequence was put forward. Firstly, the information of image to be encrypted can be encoded into two phase-only masks (POMS) for initial encryption by fractional Fourier interference. Secondly, using the wavelet digital watermarking theory, the phase masks as a watermark were embedded in the host images for re-encryption. Finally, the encrypted host images were performed pixel replacement operation to complete the entire encryption process by chaotic sequence. The encryption scheme can hide the two POMS obtained by encoding, so illegal user can not obtain the original image silhouette information by using one or two POMS. The encryption process is simple, and keys have good sensitivity. The last two step encryptions have the randomness and further improve the security and robustness of the entire encryption system. The simulation results show that the method is feasible, the image quality ideal and safety is high.

Key words: interference; image encryption; digital watermark; chaos map; fractional Fourier