DOI: 10.13382/j.jemi.2017.06.009

基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法*

肖 宁 李爱军

(山西财经大学 信息管理学院 太原 030006)

摘 要:为了解决当前光学图像加密算法因其输出密文的相位信息完全被保留在纯相位掩码中,使其出现轮廓显现问题而降低算法安全性的不足,提出了基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法。首先,引入 Gyrator 变换对明文进行处理,形成 Gyrator 变换频谱;基于离轴圆谐分量展开机制,将 Gyrator 变换频谱分割为零阶圆谐分量与非零阶圆谐分量;通过引入球面相位因子,对零阶圆谐分量进行调制,获取其相应的密文;随后,利用迭代相位检索 Gyrator 变换算法,将零阶与非零阶幅度视为输入明文与输出密文的幅度约束条件,对非零阶圆谐分量完成编码,获取一个复杂场分布,从而完成整个明文的加密。实验结果显示,与当前光学图像加密技术相比,所提算法的安全性与鲁棒稳健性更高,具有更强的抗噪声攻击与抗剪切攻击能力。所提算法能够更好地保护图像在网络中安全传输,具有较好的实用性。

关键词: 光学图像加密;圆谐分量展开;Gyrator 变换;球面相位因子;幅度约束条件;迭代相位检索

中图分类号: TP309 文献标识码: A **国家标准学科分类代码**: 520.6040

Optical image encryption algorithm based on circular harmonic component expansion and Gyrator transform domain phase retrieval

Xiao Ning Li Aijun

(College of Information management, Shanxi University of Finance and Economics, Taiyuan 030006, China)

Abstract: In order to solve the problem such as need the strict optical calibration in current optical image encryption algorithm, the optical image encryption algorithm based on circular harmonic component expansion and Gyrator transform domain phase retrieval was proposed in this paper. Firstly, Gyrator transform spectrum was formed by introducing Gyrator transform to deal with the plain. Then the spectrum of Gyrator transform is divided into zero order harmonic components and non-zero order harmonic components based on off-axis circular harmonic component expansion mechanism. The cipher was obtained by introducing the spherical phase factor to modulate the non-zero order harmonic component. Finally, the complex distribution was obtained by using the retrieval algorithm of Gyrator transform to take the zero order and non-zero order amplitude as the constraints condition of input plain and output cipher to finish the image encryption. The experimental results show that this algorithm has higher security and anti-filtering robustness with stronger anti-noise attack and anti-shear attack ability. This proposed algorithm can better protect the image in the network security transmission with good practicality.

Keywords: optical image encryption; circular harmonic component expansion; Gyrator transform; spherical phase factor; amplitude constraint; iteration phase retrieval

1 引 言

信息安全已成为当前各国的关注焦点,特别是随着计算机科学技术与互联网技术的快速发展,使得信息被窃取变得越来越容易[1]。图像作为当前人们进行沟通交流的直观载体,给当代生活带来了巨大利益,然而,由于图像包含的信息非常多,在开放网络传输中容易遭受到

收稿日期:2016-12 Received Date: 2016-12

*基金项目:国家自然科学基金(60873100)、山西省自然科学基金(2012011017-6)资助项目

外来攻击,使得相关信息被窃取,给人们带来了巨大的损失[2]。尤其是光学图像具有数量大、信息相关性高等特点,导致传统数据加密技术难以实现安全传输[3]。为此,各国学者开始设计了相应的光学图像加密技术,如姜晓洁等人[3]为了提高光学图像在开放网络中传输的安全性,提出了基于超混沌系统的光学加密技术,通过利用 Logistic 混沌序列对光学图像像素位置矩阵进行置乱操作,并借助超混沌 Chen 系统对置乱后像素的灰度值进行扩散处理,实验结果显示其算法具有良好的安全性。然而,依赖高维混沌系统对像素进行扩散会导致较高的加密耗时。为此,Liu 等人[4]为了提高光学加密技术的效率,实现实时加密,提出了基于压缩感知与分数阶傅里叶域的光学图像加密技术,引入压缩感知,对输入明文进行数据压缩,并利用基于混沌的双随机相位编码技术对压缩数据进行加密,结果显示算法具有较高的安全性与敏感性。Chen 等人[5]为实现光学图像的安全加密,设计了基于多光束干扰与矢量分解的光学图像加密技术,利用分解技术,通过将输入明文进行均等分割成两个矢量,利用多光束干涉,将输入两个矢量分别编码为幅度掩码与相位掩码,并将二者视为加密密钥,完成图像加密,实验结果显示该技术具有较高的加密安全性与抗噪声攻击能力。但是,此类基于干涉原理的光学图像加密由于其变换频谱信息被完全保留在 POMS 中,使其容易产生轮廓问题,降低算法的安全性。

为了消除轮廓问题,避免其需要严格的光学校准,本文综合圆谐分量展开与 Gyrator 变换域相位检索,设计了新的基于干涉的光学图像加密算法,将明文编码为幅度具有旋转对称结构的两个复杂场。并测试了本文光学图像加密算法的安全性与稳健性。

2　Gyrator 变换

积分变换[6]由于其含有变换参数,可以被视为加密钥,有效扩大密钥空间,在图像加密中得到广泛应用。为此,本文引入 Gyrator 变换[7],将输入明文转换为 Gyrator 变换频谱:

$$O(u,v) = g^{\alpha}\{o(x,y)\}(u,v) = \frac{1}{|\sin\alpha|}\iint o(x,y)\exp\left(\mathrm{j}2\pi\frac{(uv+xy)\cos\alpha-(xv+yu)}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \tag{1}$$

式中:$g^{\alpha}(\,)$ 代表变换角度为 α 的 Gyrator 变换算子,(x,y) 是输入坐标,(u,v) 是输出坐标,$o(x,y)$ 代表复杂场函数。而 $g^{\alpha}(\,)$ 的逆变换 $|o_0|$ 为:

$$g^{-\alpha}(o(x,y)) = g^{2\pi-\alpha}(o(x,y)) \tag{2}$$

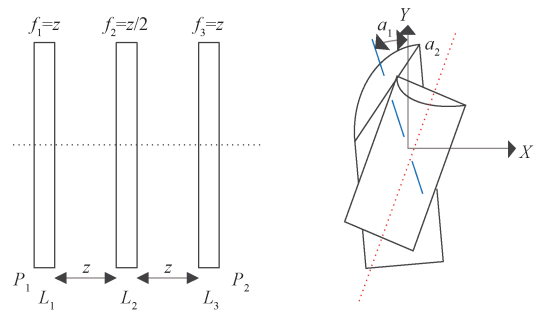
本文通过利用 Gyrator 变换的 3 个广义透镜的级联结构对图像进行加密,如图 1 所示。图 1(a)的 3 个广义透镜组合成光学系统;任意两个透镜之间的距离是相等的,均为 Z。另外,透镜 L_1 与 L_2 的焦距均是 Z;而 L_2 的焦距为 $\frac{Z}{2}$。且 P_1、P_2 分别代表输入、输出平面。图 1(b)是广义透镜的结构,α_1、α_2 均为旋转角度,满足:

$$\alpha_1 = -\alpha;\alpha_2 = \alpha - \pi/2 \tag{3}$$

明文图像由 P_1 平面进入,通过图 1(a)显示的 GT 光学系统处理后,可在 P_2 平面获取变换频谱:

$$O(u,v) = \frac{1}{|2\lambda\sin\alpha_2|}\times\iint o(x,y)\exp\left(\mathrm{j}2\pi\frac{(uv+xy)(2\sin2\alpha_1\sin2\alpha_2-1)-\frac{(xv+yu)}{2\lambda z\sin2\alpha_2}}{\sin\alpha}\right)\mathrm{d}x\mathrm{d}y \tag{4}$$

其中,λ 是光波波长。



(a) 光学系统　(b) 广义透镜
(a) Optical system　(b) Generalized lens

图 1　*Gyrator* 变换的光学系统
Fig. 1　Optical system of Gyrator transform

3　本文光学图像加密算法设计

令 $o(x_0,y_0)$ 是初始明文的归一化强度分布,则通过一个纯相位掩码 POM(phase - only mask)对其进行调制:

$$o'(u,v) = \sqrt{o(x_0,y_0)}\exp[\mathrm{j}2\pi\, rand(x_0,y_0)] \tag{5}$$

式中:$rand(\,) \in [0,1]$ 代表一致分布的随机函数。对于输入明文来说,其坐标点 $(0,0)$ 是位于图像中心处,则仪器光轴将在解密平台上通过此点。再根据旋转角为 $-\alpha$ 的可逆 Gyrator 变换,对调制图像 $o'(x_0,y_0)$ 进行处理:

$$m(x_1,y_1) = g^{-\alpha}\{o'(x_0,y_0)\} = |m(x_1,y_1)|\exp[\mathrm{j}\varphi_m(x_1,y_1)] \tag{6}$$

式中:$|\ |$ 代表模运算,$\varphi(x_1,y_1)$ 是可逆 Gyrator 变换频谱相。

根据文献[8]可知,当前基于干涉原理的光学图像加密算法之所以存在轮廓问题,主要是由 $m(x_1,y_1)$ 的相位信息引起的。为了降低 $\varphi_m(x_1,y_1)$ 的单边效应,本文

将另外一个随机相位掩码 RPM(random phase mask) $\exp[\mathrm{j}\varphi(x_1,y_1)]$引入到 $m(x_1,y_1)$ 中,对其进行平滑:

$$m(x_1,y_1) = |m(x_1,y_1)|\exp[\mathrm{j}\phi(x_1,y_1)]\cdot \exp\{\mathrm{j}[\varphi_m(x_1,y_1)-\phi(x_1,y_1)]\} = D(x_1,y_1)P_1(x_1,y_1) \tag{7}$$

$$D(x_1,y_1) = |m(x_1,y_1)|\exp[\mathrm{j}\phi(x_1,y_1)] \tag{8}$$

$$P_1(x_1,y_1) = \exp\{\mathrm{j}[\varphi_m(x_1,y_1)-\phi(x_1,y_1)]\} \tag{9}$$

式中:$\phi(x_1,y_1)\in[0,2\pi]$ 是随机相位分布。根据模型(7)可知,相位信息 $\varphi_m(x_1,y_1)$ 并不仅保留在 $D(x_1,y_1)$,从而消除了轮廓问题。

随后,基于离轴圆谐分量展开机制,将 $D(x_1,y_1)$ 展开为一系列的圆谐分量。本文随机选择一个离轴位置 (a,b) 作为圆谐分量展开的中心,为了计算该圆谐分量,首先将坐标系统转换为 $x'_1 = x_1 + a$,$y'_1 = y_1 + b$。因此,在新的坐标系统中,$D(x_1,y_1)$ 演变为 $D(x_1+a,y_1+b)$,再根据如下规则,将 Cartesian 坐标变成极坐标:

$$\begin{cases} x' = r\cos\theta \\ y' = r\sin\theta \end{cases} \tag{10}$$

根据式(10)可知,在极坐标中,$D(x_1,y_1)$ 演变为 $D(r\cos\theta+a,r\sin\theta+b)$,因此,位置在 $r=0$,$\theta=0$ 处的圆谐分量展开机制为:

$$D(r\cos\theta+a,r\sin\theta+b) = D(r,\theta) = \sum_{n=-\infty}^{+\infty} o_n(r)\exp(\mathrm{j}n\theta) = \sum_{n=-\infty}^{+\infty} C_n(r,\theta) \tag{11}$$

其中,$C_n(r,\theta) = o_n(r)\exp(\mathrm{j}n\theta)$ 是第 n 阶圆谐分量展开。$o_n(r)$ 为:

$$o_n(r) = \frac{1}{2\pi}\int_0^{2\pi} D(r,\theta)\exp(-\mathrm{j}n\theta)\mathrm{d}\theta \tag{12}$$

根据式(11)、(12)可知,所有的圆谐分量都是旋转对称的。另外,根据式(12)可知,$o_n(r)$ 严重依赖对称中心的坐标位置,有效提高算法的安全性。随后,本文将 $D(x_1,y_1)$ 分割为零阶圆谐分量与非零阶圆谐分量:

$$D(r\cos\theta+a,r\sin\theta+b) = C_0(r,\theta)+C'(r,\theta) \tag{13}$$

$$C_0(r,\theta) = o_0(r) = |o_0(r)|\exp[\mathrm{j}\varphi_{o_0}(r)] \tag{14}$$

$$C'(r,\theta) = |C'(r,\theta)|\exp[\mathrm{j}\varphi_{C'}(r)] \tag{15}$$

式中:$C_0(r,\theta)$ 代表零阶圆谐分量,$C'(r,\theta)$ 代表非零阶圆谐分量。

为了进一步改善算法的安全性,本文引入相位球面因子 $U(x_1,y_1)$,对零阶圆谐分量 $C_0(r,\theta)$ 进行调制:

$$o_0(r)U(x_1,y_1) = |o_0(r)|\exp[\mathrm{j}\phi_{o_0}(r)]\exp\left[\mathrm{j}\frac{k}{2Z}(x_1^2+y_1^2)\right] \tag{16}$$

$$r = \sqrt{(x_1-a)^2-(y_1-b)^2} \tag{17}$$

式中:r 代表极坐标,$k = 2\pi/\lambda$ 是波矢量,λ 是照明光的波长,z 是球面波的半径。

再通过乘以式(16)的相位部分,可得纯相位密钥 K_1:

$$K_1(x_1,y_1) = \exp[\mathrm{j}\phi_{o_0}(r)]\times U(x_1,y_1)\times P_1(x_1,y_1) \tag{18}$$

接下来,本文利用迭代相位检索算法[9]与 Gyrator 变换来编码非零阶圆谐分量,如图 2 所示。通过相位截断与幅度截断,分别提取幅度部分 $C'(r,\theta)$ 与相位部分 $\exp[\mathrm{j}\varphi_{C'}(r,\theta)]$。在迭代过程中,幅度分量 $C'(r,\theta)$ 与零阶幅度 $o_0(r)$ 被视为 Gyrator 变换计算中输入、输出平面的幅度约束条件。但是在 Cartesian 坐标系统中,两个幅度约束条件分别为:

$$\left|C''\left[\sqrt{(x_1-a)^2+(y_1-b)^2},\tan^{-1}\frac{y_1-b}{x_1-a}\right]\right|,\ \left|o_0\sqrt{(x_2-a)^2+(y_2-b)^2}\right| \tag{19}$$

式中:(x_2,y_2) 是输出平面的坐标。

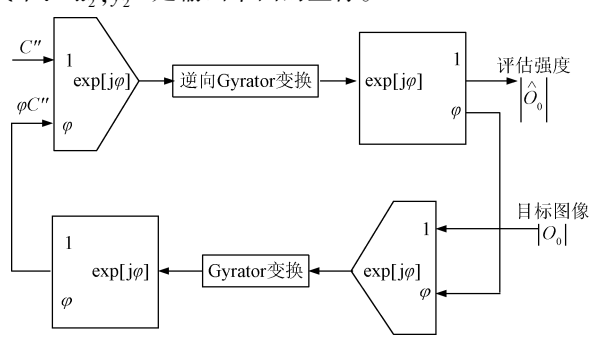


图 2　迭代相位检索 Gyrator 变换算法流程

Fig. 2　Flow path of phase retrieval Gyrator transformation algorithm

变换角度为 $-\beta$ 时的可逆 Gyrator 变换是通过执行一个复杂函数来启动迭代过程,其产生的频谱幅度则被 $|o_0|$ 代替,再执行变换角度为 β 时的 Gyrator 变换。那么约束幅度 $|C''|$ 乘以更新后的相位分布就是可逆 Gyrator 变换。通过反复执行以上过程,直到目标图像 $|o_0|$ 与近似目标 $|\hat{o}_0|$ 的相关系数达到 0.999 99[10]。故本文利用相关系数 ρ 来控制迭代数量:

$$\rho = \frac{E\{[T-E(T)]\times[\hat{T}-E(\hat{T})]\}}{E\{[T-E(T)]^2\times E\{[\hat{T}-E(\hat{T})]^2\}\}^{1/2}} \tag{20}$$

式中:T 是迭代算法的目标图像,$\hat{T}$ 是近似目标图像,E 代表期望算子。

根据式(20),当 $\hat{T}$ 与 T 非常接近时,ρ 值达到最大。则相应的 Gyrator 变换关系为:

$$g^{-\beta}\{o'\}\exp[\mathrm{j}\varphi_{C''}(x_1,y_1)] = |\hat{o}_0|\exp[\mathrm{j}\varphi_{Ck}(x_2,y_2)] \tag{21}$$

其中，$\exp[\mathrm{j}\varphi_{C''}(x_1,y_1)]$ 和 $\exp[\mathrm{j}\varphi_k(x_2,y_2)]$ 是迭代过程中产生的两个纯相位函数。

由于幅度 $|\hat{o}|$ 与约束图像 $|o_0|$ 是很相似，因此，可以直接使用 $|o_0|$ 替代 $|\hat{o}|$，对初始明文进行检索。随后，将式(21)中的目标图像的相位部分与 1 个球面相位函数进行乘法运算，得到新的纯相位密钥 $K_2(x_2,y_2)$：

$$K_2(x_2,y_2) = \exp[\mathrm{j}\varphi_k(x_2,y_2)]U(x_2,y_2) = \exp[j\varphi_k(x_2,y_2)]\exp\left[\mathrm{j}\frac{k}{2z}(x_2^2+y_2^2)\right] \tag{22}$$

再联合式(9)中的 $P_1(x_1,y_1)$ 与 $\exp[\mathrm{j}\varphi(x_1,y_1)]$，得到第 3 个纯相位密钥 $K_3(x_3,y_3)$：

$$K_3(x_3,y_3) = \exp[\mathrm{j}\varphi_{C''}(r,\theta)-\mathrm{j}\varphi_{C''}(x_1,y_1)]P_1(x_1,y_1) \tag{23}$$

综合式(18)、(22)与(23)，可以产生 3 个纯相位密钥 $K_1(x_1,y_1)$、$K_2(x_2,y_2)$、$K_3(x_3,y_3)$，以及真实的密文 $|o_0|$。这 3 个纯相位密钥则可用于算法的解密密钥，其解密过程中的光电混合结构如图 3 所示。通过两个空间光调制器 SLM_1、SLM_2，两个相同的密文被显示在两个干涉分支的输入平面内。通过将零阶圆谐分量视为参考位置，从而有效解决校准问题。另外两个空间光调制器 SLM_3、SLM_4 排在 SLM_1、SLM_2 后面，分别显示密钥 $K_1(x_1,y_1)$、$K_2(x_2,y_2)$。

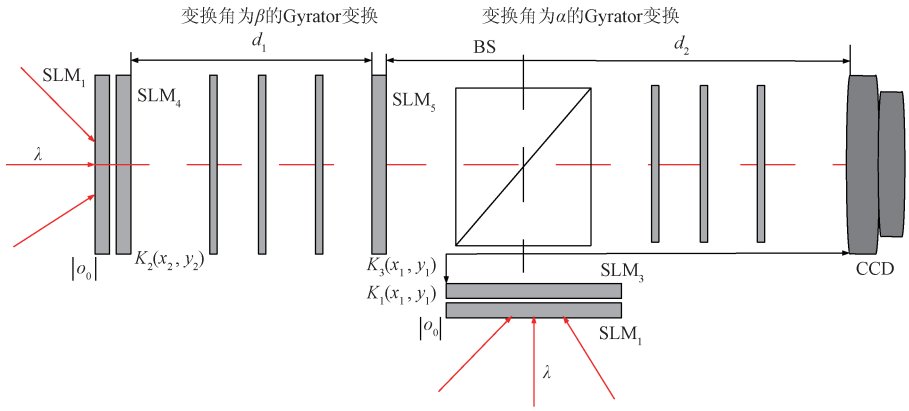


图 3　解密过程的光电混合结构

Fig. 3　The photoelectric hybrid structure of decryption process

再根据纯相位密钥 $K_1(x_1,y_1)$，其第 1 个 $SLM(SLM_1,SLM_3)$ 组合的衍射波为：

$$M_1(x_1,y_1) = |o_0|K_1(x_1,y_1)\times U(x_1,y_1) = o_0(r)P_1(x_1,y_1) \tag{24}$$

对于另外 1 个干涉分支，利用变换角为 β 的光学 Gyrator 变换，在第 2 个 $SLM(SLM_2,SLM_4)$ 组合后，对衍射函数进行编码。然后利用显示在空间光调制器 SLM_5 中的纯相位密钥 $K_3(x_3,y_3)$ 对输出结果进行调制：

$$M_2(x_1,y_1) = g^{\beta}\{|o_0|\times K_2(x_2,y_2)\times U(x_2,y_2)\}\times K_3(x_1,y_1) = C''(r,\theta)\times P_1(x_1,y_1) \tag{25}$$

再借助一个分束器与变换角为 α 的 Gyrator 变换，两个衍射光束就被组合在一起。最后，通过位于输出平面上的 CCD，记录解密图像：

$$R(x_0,y_0) = |g^{\alpha}\{M_1(x_1,y_1)+M_2(x_1,y_1)\}|^2 \tag{26}$$

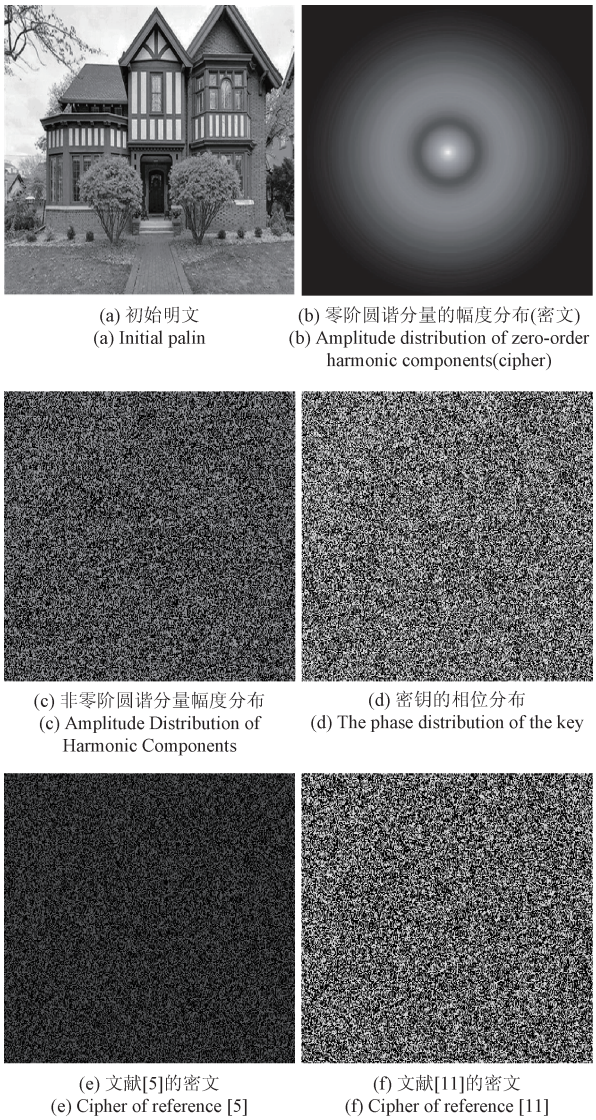
根据上述内容可知，攻击者在没有得到正确的纯相位密钥与额外的附加密钥(旋转中心 (a,b) 的相对位置、变换角 α 与 β、球面，球面波的波长与半径)情况下，是无法检索到正确的密文。

4　实验结果与分析

为了验证所提光学图像加密技术的合理性与优异性，在 MATLAB 6.5 中进行测试，同时，将当前加密性能较好的算法视为对照组：文献[5,11]。其中，文献[5]是设计多光束干扰与矢量分解的光学图像加密技术，利用普通分解技术，通过将输入明文进行均等分割成两个矢量，通过多光束干涉，将输入两个矢量分别编码为幅度掩码与相位掩码；文献[11]则是利用涡流环形光束干扰与菲涅尔变换来实现光学加密，将输入明文调制为输入平面上的相位掩码，以及频域面上的幅度掩码，将幅度掩码视为密文。算法参数为 Gyrator 变换角 $\alpha = 1.721$，$\beta = 2.058$，波长 $\lambda = 623.8$ nm，球面波的半径 $z = 0.06$ m。通过 Gyrator 变换与随机相位调制处理，根据初始明文，可生成复杂变换频谱 $D(x_1,y_1)$，且圆谐分量的扩展中心在离轴位置 $(x_1 = 2, y_1 = 2)$ 处。

4.1　光学图像加密效果

以图 4(a)所示为测试对象，利用本文算法、文献[5,11]对其进行光学加密，结果如图 4(b)~(f)所示。



(a) 初始明文
(a) Initial palin

(b) 零阶圆谐分量的幅度分布(密文)
(b) Amplitude distribution of zero-order harmonic components(cipher)

(c) 非零阶圆谐分量幅度分布
(c) Amplitude Distribution of Harmonic Components

(d) 密钥的相位分布
(d) The phase distribution of the key

(e) 文献[5]的密文
(e) Cipher of reference [5]

(f) 文献[11]的密文
(f) Cipher of reference [11]

图4　3种光学加密算法的输出密文

Fig. 4　Output cipher of three optical encryption algorithms

根据测试结果可知,从视觉上看,3种光学加密技术都具有良好的保密效果,明文的信息被彻底混淆,攻击者无法从其获取任何信息,分别如图4(b)、(e)、(f)所示。为了量化3种加密技术的优异,本文引用信息熵值[12]来衡量,评估结果见表1。根据表可知,本文算法输出的密文熵值约为7.995 2,与理论值8非常接近,这显示所提算法出现信息泄露的概率可以忽略。而文献[5,7]两种技术的熵值分别为7.990 8、7.987 5,均要低于所提算法,这显示两种加密技术的安全性要低于本文加密技术。可见,本文算法的安全性比文献[5,7]要略高。原因是本文算法利用了离轴圆谐分量展开机制将Gyrator变换频谱分割为零阶、非零阶圆谐分量,并利用球面相位因子,对零阶圆谐分量进行调制,形成相应的密文,使其相位信息并不保留在POMS中,消除了轮廓问题,即使攻击者知道其中一个相位板,也是无法看到输入明文的轮廓信息;且通过将其分割为零阶、非零阶圆谐分量,并引入球面因子,分别对其进行调制与编码处理,显著增大了算法的密钥空间,在整体上,使得所提算法的安全性要高于对照组。而文献[5,7]这两种光学加密技术通过光干涉原理实现明文加密,但是二者的最大缺点就是其密文的相位信息完全保留在POMS中,使其轮廓问题较为显著,攻击者通过任何一个相位板就可以获得输入明文的轮廓信息,一定程度上削弱了安全的安全性。

表1　信息熵值测试测试果

Table 1　Test results of information entropy

名称	本文算法	文献[5]	文献[11]
密文熵值	7.995 2	7.990 8	7.987 5

4.2　密钥敏感性测试

良好的加密算法应满足严格的“雪崩效应”,即使密钥发生极其微小的变化,攻击者也是无法得到正确的解密图像[13]。为此,本文测试了Gyrator变换角 $\alpha = 1.721$ 的敏感性,利用偏差 $\Delta t = 10^{-16}$ 对 $\alpha = 1.721$ 进行变动,得到新的密钥参数 $\alpha' = 1.721 + 10^{-16}$,其余密钥均不变。从而利用这组新密钥对图4(b)进行解密,获得解密结果与其均方差(MSE)曲线如图5所示。依图5可知,即使 $\alpha = 1.721$ 变为 $\alpha = 1.7\ 210\ 000\ 000\ 000\ 001$,其 *MSE* 值发生突变,由57.91扩大为3 265.75,远超过解密阈值(理论值为3 000[14])。可见,本文算法具有较强的密钥敏感性,即使密钥发生 $\Delta t = 10^{-16}$ 这样的微小偏差,所得到的解密数据是截然不同的,具备理想的“雪崩效应”。

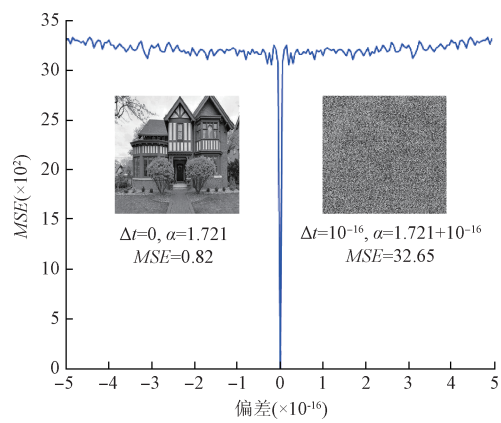


图5　本文算法的密钥敏感性测试

Fig. 5　Key sensitivity test of the algorithm in this paper

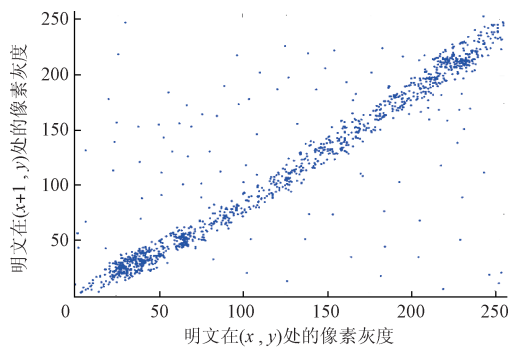
4.3　相邻像素点的相关性对比测试

图像相邻像素之间的强烈相关性对其信息安全威胁较大,这种特性易被攻击者利用,从而破译密文,理想的

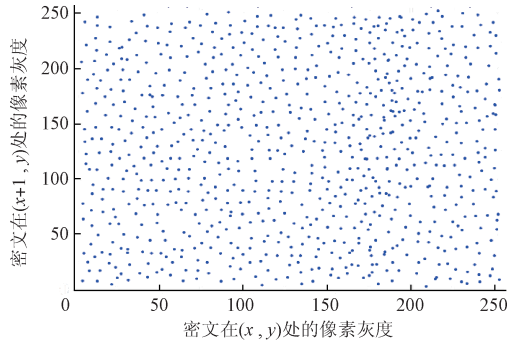
加密算法可以消除这相关性[15]。在图 4(a)、(b)、(e) ~ (f)中分别择取 3 000 对相邻像素点,根据式(27)来计算该系数 T_{xy}[15]。

$$T_{xy}=\frac{1/n\sum_{i=1}^{n}(x_i-E(x_i))(y_i-E(y_i))}{\sqrt{\left(1/n\sum_{i=1}^{n}(x_i-E(x_i))^2\right)\left(1/n\sum_{i=1}^{n}(y_i-E(y_i))^2\right)}} \tag{27}$$

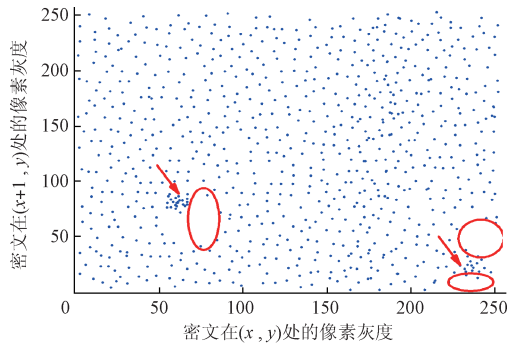
依据式(27),获取的明文与所提算法、文献[5,7]的加密密在水平方向上的 T_{xy} 值如图 6 所示。根据图 6(a)的数据,未加密之前的明文中任意两相邻像素之间的 T_{xy} 值较高,其像素分布近似对角线,T_{xy} 值约为 0.967 2;但是利用所提加密技术与文献[5,11]处理后,这种强烈相关性的得到了显著降低,如图 6(b) ~ (d)所示。然而,本文算法输出密文的像素灰度分布最为均匀,其相邻像素相关性最小,其 T_{xy} = 0.001 6,如图 6(b)所示。而文献[5,11]的输出密文相对明文而言,其相邻像素相关性也得到了极大的削弱,T_{xy} = 0.002 3、0.003 7,但是其密文的像素灰度分布均匀度低于所提算法,均存在一定的“像素聚堆”与“空洞效应”,降低图像像素分布的随机度,使得二者的抗统计攻击能力要弱于本文算法,分别见图 6(c) ~ (d)中的箭头与圈圈所指。其余两个方向的 T_{xy} 数据见表 2。根据表中数据,对于 3 个方向的 T_{xy} 值,明文之间的相关系数值要显著大于加密后的密文,且本文算法的密文相关系数始终是最低的。原因是本文加密技术将球面相位因子嵌入到零阶圆谐分量中对其完成调制来获取相应的密文,改变了图像的像素值,并使其相位信息并不保留在 POMS 中,避免信息外漏,并利用迭代相位检索 Gyrator 变换技术来编码非零阶圆谐分量,形成一个旋转对称结构的复杂场,从而使得算法具有理想的安全性,最大程度降低这种相邻像素相关性,使其像素灰度分布更加均匀,这种均匀的像素灰度分布显著增强了算法的随机度,从而改善了地改善了算法的抗统计攻击能力。而文献[5,11]是采用光干涉原理实现明文加密,虽然对像素位置与像素值进行了扩散,但是输出密文的信息集中在一个 POMS 中,不能有效解决图像轮廓问题,在其解密过程中,攻击者可以根据其轮廓信息来检索图像中像素位级的某些信息,使得算法的安全度与随机度不理想,削弱了算法的抗统计攻击能力。



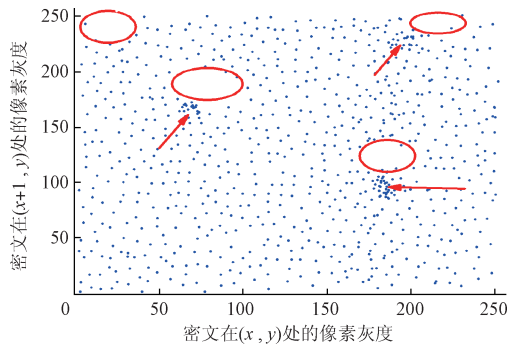
(a) 明文
(a) Plain image



(b) 本文算法的密文
(b) Cipher of this algorithm



(c) 文献[5]的密文
(c) Cipher of reference [5]



(d) 文献[11]的密文
(d) Cipher of reference [11]

图 6　本文算法的相邻像素之间的相关性测试

Fig. 6　Correlation test between adjacent pixels of the algorithm in this paper

表 2　3 个方向的相关性测试

Table 2　Correlation test of three directions

名称	图 7(b)	图 7(c)	图 7(d)	明文
水平	0.001 6	0.002 3	0.003 7	0.967 2
垂直	0.002 8	0.005 4	0.007 3	0.969 8
对角线	0.003 5	0.006 9	0.009 1	0.982 2

4.4　加密算法的鲁棒性测试对比分析

在图像处理和传输过程中都会有噪声的影响，故加密技术应具备较高的抗噪声攻击能力[16]。对此，本文将方差为0.3的高斯噪声施加于图5(b)，则相应的噪声干扰密文变成：

$$E' = E(1 + KN) \tag{28}$$

式中：E'为噪声干扰密文，k是噪声强度系数，N为高斯噪声。

在噪声攻击环境下的密文解密结果如图7所示。可见，随着k值的增大，其解密图像的MSE值越大，且3种算法的都具有较好的抗噪声攻击能力，但是本文光学加密技术的鲁棒性更强，当$k = 1$时，本文算法的解密图像的MSE值要低于文献[5,11]，分别为768、907、1 124，三者均要远低于解密阈值3 000。这显示本文光学加密技术具有更高的抗噪声攻击能力。

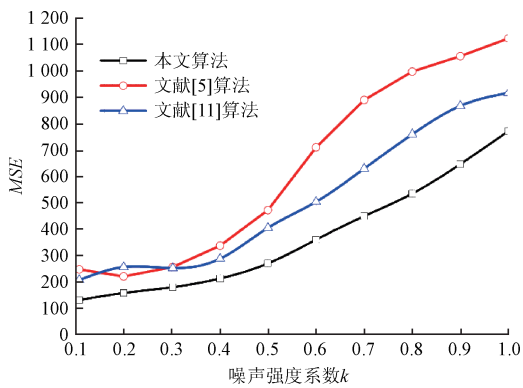
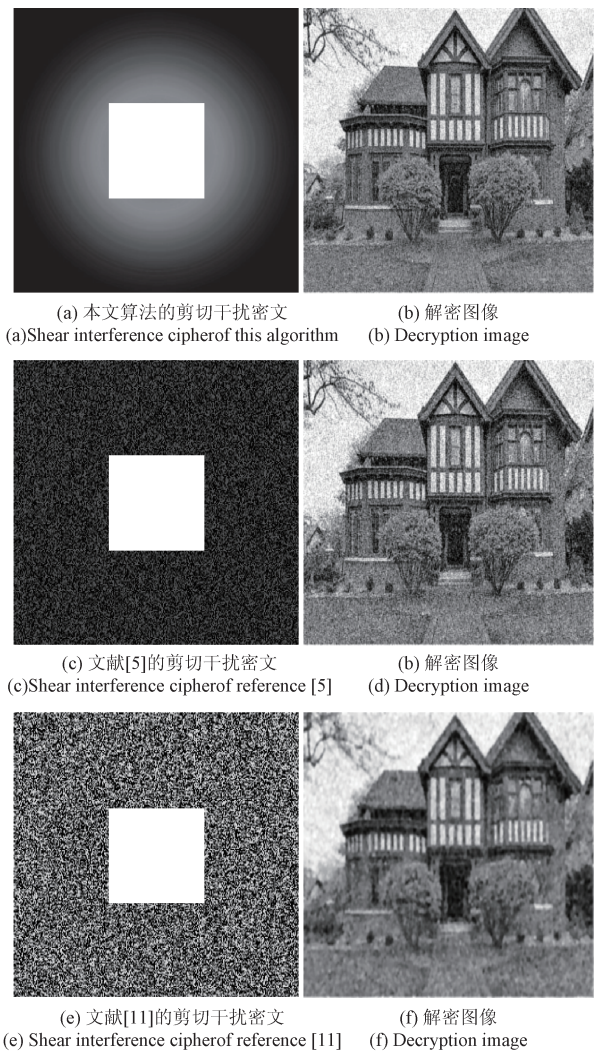


图7　3种算法的抗噪声攻击能力测试

Fig. 7　Anti-noise attack ability test of three algorithms

剪切攻击也是衡量加密技术鲁棒性的重要指标[17]，因此，本文将图4(b)、(e)、(f)视为样本，对三者施加的1/4剪切干扰，如图8(a)、(c)、(e)所示，再利用3种算法对其完成解密，输出数据如图8(b)、(d)、(f)所示。根据图8可知，在图像遭遇剪切攻击时，本文光学加密机制表现出更强的抗剪切攻击性能，输出图像较好地保留了明文的信息，与明文的相似度最高，如图8(b)所示，而文献[5,11]两种算法的解密结果不佳，虽然将密文破译了，但是输出图像信息存在丢失，不能完整的复原明文，如图8(d)、(f)所示。主要原因是所提光学加密算法通过离轴圆谐分量展开机制将Gyrator变换频谱分割为零阶、非零阶圆谐分量，并结合球面相位因子对零阶圆谐分量进行调制，使得密文的相位信息并不保留在纯相位掩码中，避免了轮廓问题，有效降低了密文中相邻像素间的相关性，使得像素灰度分布更加均匀与更高的随机度，另外，整个图像的信息随机分散在几个相位板上，当攻击者剪切一小部分信息时，使得图像内容损失最小，从而增强了算法的剪切攻击能力。而文献[5,11]这两种光学加密技术虽然也具有一定的抗剪切攻击能力，但是其密文的相位信息完全保留在纯相位掩码中，当攻击者剪切一小部分信息时，二者的图像信息缺失程度要高于所提算法，且由于这两种算法均是采用光干涉原理，虽然降低了密文中相邻像素间的相关性，但是密文中存在“像素聚堆”与“空洞效应”，使得像素分布均匀程度不理想，从而使其密文的抗剪切攻击能力较低。



(a) 本文算法的剪切干扰密文　(b) 解密图像
(a)Shear interference cipherof this algorithm　(b) Decryption image

(c) 文献[5]的剪切干扰密文　(b) 解密图像
(c)Shear interference cipherof reference [5]　(d) Decryption image

(e) 文献[11]的剪切干扰密文　(f) 解密图像
(e) Shear interference cipherof reference [11]　(f) Decryption image

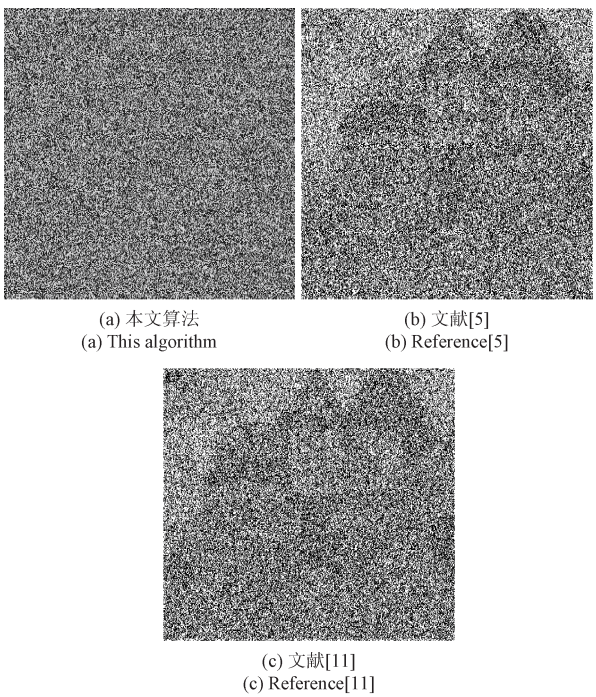
图8　3种加密算法的抗剪切攻击能力

Fig. 8　Anti-shear attack test of three algorithms

4.5　算法的轮廓显现问题

基于干涉原理的光学图像加密技术易出现“轮廓显现”问题，也就是黑客只要随机取一个相位板放在解密光路中，便可轻而易举地获得明文轮廓信息[18]，从而降低了算法的安全性。从本文算法、文献[5,11]中取出一个相位板，其中，本文算法单独使用$K_1(x_1, y_1)$、文献[5]使用其相位板P_1、文献[11]单独使用其相位板T_1，利用各

自的解密机制对图 4(b)、(e)、(f)进行解密,结果如图 9 所示。依该图测试结果可知,单独使用相位板 $K_1(x_1,y_1)$ 所获得的解密图像无法显示其轮廓,而文献[5,11]两种技术的解密结果虽然许多噪声点干扰,但是明文的轮廓信息被泄露出来。原因是本文算法将随机相位掩码 $\exp[j\phi(x_1,y_1)]$ 引入到 $m(x_1,y_1)$ 中,从而导致相位信息 $\varphi_m(x_1,y_1)$ 并不保留在纯相位掩码 $D(x_1,y_1)$ 中(式(7)),从而消除了轮廓问题。而文献[5,11]这两种技术则是单纯利用相位信息进行调制,从而导致相位信息被完全保留在其纯相位掩码中,存在一定的轮廓问题。



(a) 本文算法
(a) This algorithm

(b) 文献[5]
(b) Reference[5]

(c) 文献[11]
(c) Reference[11]

图 9　3 种算法的轮廓显现问题测试

Fig. 9　Contour show problem test of three algorithms

5　结　论

为了解决当前光学图像加密存在的轮廓显现问题,提高算法的鲁棒性与安全性,本文提出了基于圆谐分量展开与 Gyrator 变换域相位检索的光学图像加密算法。通过该算法,输入明文被编码为两个复杂场函数。利用离轴圆谐分量展开机制对 Gyrator 变换频谱进行分割为零阶圆谐分量与非零阶圆谐分量,并利用相位迭代检索算法将非零阶圆谐分量进行编码,通过将编码的图像的幅度约束为零阶圆谐分量的幅度,从而将最终得到的零阶圆谐分量的幅度视为密文。实验结果显示:所提算法具有更高的安全性与鲁棒性更高,有效消除了轮廓问题。

参考文献

[1] 李湘锋, 赵有健, 全成斌. 对称密钥加密算法在 IPsec 协议中的应用[J]. 电子测量与仪器学报, 2015, 28(1): 75-82.
LI X F, ZHANG Y J, QUAN CH B. Application of symmetric key encryption algorithm in IPsec protocol [J]. Journal of Electronics Measurement & Instrumentation, 2015, 28 (1): 75-82.

[2] YE G D, WONG K W. An image encryption scheme based on time-delay and hyper-chaotic system [J]. Nonlinear Dynamics, 2013, 71 (1): 259-267.

[3] 姜晓洁,谢永超. 基于超混沌系统的光学图像加密算法[J]. 激光杂志,2015,36(6):68-71.
JIANG X J, XIE Y CH. Optical image encryption algorithm based on hyper-chaotic system [J]. Laser Journal,2015,36(6):68-71.

[4] LIU X B, MEI W B, DU H Q. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain [J]. Journal of Modern Optics, 2014, 61 (19): 1570-1577.

[5] CHEN L F, HE B Y, CHEN X D. Optical image encryption based on multi-beam interference and common vector decomposition [J]. Optics Communications, 2015, 361(2): 6-12.

[6] 刘兴斌. 基于分数 Sumudu 变换和分数梅林变换的图像加密算法研究[D]. 南昌:南昌大学,2012: 22-23.
LIU X B. Research on image encryption algorithm based on fractional sumudu transform and fractional merlin transform [D] Nanchang: Nanchang University, 2012; 22-23.

[7] 林睿. Gyrator 变换全息图及其在图像加密中的应用[J]. 光子学报, 2013, 42(2): 123-130.
LIN R. Gyrator transform hologram and its application in image encryption [J]. Acta Photonica Sinica, 2013, 42(2): 123-130.

[8] WANG X, ZHAO D. Optical image hiding with silhouette moval based on the optical interference principle [J]. Application Optical, 2013, 51 (8): 686-691.

[9] YAO L L, YUAN C J, QIANG J J. An asymmetric color image encryption method by using deduced gyrator transform[J]. Optics and Lasers in Engineering, 2016, 89(2): 72-79.

[10] HWANG H E, CHANG H T, LIE W N. Multiple-image encryption and multiplexing using modified Gerchberg-Saxton algorithm and phase modulation in Fresnel transform domain [J]. Optics Letters, 2015, 38 (7): 3917-3919.

[11] SINGH H, YADAV A K, VASHISTH S. Optical image encryption using Devil's vortex toroidal lens in the fresnel transform domain [J]. International Journal of Optics, 2015, 129(10): 101-109.

[12] 张庆龙, 张辉, 毛征. 基于TMS320C6455的目标跟踪系统设计与实现[J]. 国外电子测量技术, 2015, 38(5): 75-78.
ZHANG Q L, ZHANG H, MAO ZH. Design and implementation of target tracking system based on TMS320C6455 [J]. Foreign Electronic Measurement Technology, 2015, 38 (5): 75-78.

[13] 侯俊峰, 黄素娟, 司徒国海. 非线性光学图像加密[J]. 光学学报, 2015, 35(8):85-90.
HOU J F, HUANG S J, SITU G H. Nonlinear optical image encryption [J]. Editorial Office of Optics, 2015, 35 (8): 85-90.

[14] 张文全,张烨. 基于随机分数梅林变换的光学图像加密[J]. 光学精密工程, 2014, 22(3): 754-759.
ZHANG W Q, ZHANG Y. Optical image encryption based on random fractional merlin transformation [J]. Editorial Office of Optics and Precision Engineering, 2014, 22 (3): 754-759.

[15] CHEN L F, HE B Y, CHEN X D. Optical image encryption based on multi-beam interference and common vector decomposition [J]. Optics Communications, 2016, 361(15): 6-12.

[16] 汤一彬, 徐宁, 姚澄. 基于旋转不变稀疏表示和流形学习的图像降噪[J]. 仪器仪表学报, 2014, 35(5): 1101-1108.
TANG Y B, XU N, YAO CH. Image denoising based on rotational invariant sparse representation and manifold learning [J]. Instrumentation, 2014, 35 (5): 1101-1108.

[17] 涂正武, 金聪. 适用于Android手机的像素异或图像分块加密算法[J]. 电子测量技术, 2015, 38(10): 46-52.
TU ZH W, JIN C. Applicable to pixel exclusive or image block encryption algorithm for android phones [J]. Electronic Measurement Technology, 2015, 38 (10): 46-52.

[18] 汪小刚. 基于双随机相位编码和干涉原理的图像加密技术研究[D]. 杭州:浙江大学,2013: 59-60.
WANG X G. Research on image encryption technology based on dual random phase coding and interference [D]. Hangzhou: Zhejiang University, 2013: 59-60.

作者简介

肖宁,1968年出生,1990年于太原重型机械学院获得学士学位,1997年于太原理工大学获得硕士学位,现为山西财经大学讲师,主要研究方向为计算机图形图像、模式识别、信号处理。
E-mail:XiaoNing1968scdf@163.com

Xiao Ning was born in 1968, and received B. Sc. form Taiyuan Heavy Machinery College in 1990 and M. Sc. form Taiyuan University of Technology in 1997, respectively. Now he is lecturer in Shanxi Finance University. His main research interest includes computer graphics, pattern recognition, and signal processing.

李爱军,1964年出生,1985年于太原理工大学获得学士学位,1991年于中北大学获得硕士学位,2005年于北京交通大学获得博士学位,现为山西财经大学教授,硕士生导师,主要研究方向为模式识别、图像处理、信号检测。

Li Aijun was born in 1964, and received B. Sc. form Taiyuan University of Technology in 1985, M. Sc. form Zhongbei University in 1991, and Ph. D. form Beijing Jiaotong University in 2005, respectively. Now he is professor and M. Sc. tutor in Shanxi Finance University. His main research interest includes pattern recognition, image processing, and signal detection.