物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于gyrator变换和矢量分解的非对称图像加密方法

姚丽莉 袁操今 强俊杰 冯少彤 聂守平

Asymmetric image encryption method based on gyrator transform and vector operation

Yao Li-Li Yuan Cao-Jin Qiang Jun-Jie Feng Shao-Tong Nie Shou-Ping

引用信息 Citation: Acta Physica Sinica, 65, 214203 (2016) DOI: 10.7498/aps.65.214203
在线阅读 View online: http://dx.doi.org/10.7498/aps.65.214203
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2016/V65/I21

基于gyrator变换和矢量分解的非对称图像加密方法*

姚丽莉 袁操今† 强俊杰 冯少彤 聂守平

(南京师范大学, 江苏省光电技术重点实验室, 南京 210023)

(2016年6月15日收到; 2016年7月6日收到修改稿)

本文结合矢量分解和gyrator变换的数学实现得到了一种新的非对称图像加密算法, 它将待加密图像先通过矢量分解加密到两块纯相位板中, 然后利用从gyrator变换的数学实现中推导出来的加密算法加密其中一块相位板, 获得最终的实值密文. 另一块相位板作为解密密钥. 算法的解密密钥不同于加密密钥, 实现了非对称加密, 加密过程中产生的两个私钥增大了算法的安全性. 数值模拟结果验证了该算法的可行性和有效性.

关键词: gyrator变换, 非对称加密, 矢量分解, 实值密文

PACS: 42.30.–d, 42.30.Kq, 42.30.Va **DOI:** 10.7498/aps.65.214203

1 引 言

计算机和网络技术迅猛发展, 信息安全技术已经成为当今社会中保护信息传输和存储的关键技术, 图像加密技术是信息安全技术领域的重要课题. 自从Refregier和Javidi在1995年提出双随机相位加密技术[1]以来, 光学加密的相关理论和技术已经得到了快速发展, 许多光学加密方案相继被提出[2−7]. 然而, 大多数已提出的基于变换域的加密系统(例如傅里叶变换[2], gyrator变换[3]、菲涅耳变换[4]等)都是线性对称加密系统, 加密密钥与解密密钥相同, 这样的加密系统安全性不高, 容易遭到攻击[8−10]. 因此, Qin和Peng[11]在2010年提出了基于切相傅里叶变换的光学非对称密码系统, 通过在光学加密过程中引入相位截断操作, 去除了双随机相位加密系统的线性特点. 然而, 基于切相傅里叶变换的非对称密码系统容易遭到特殊攻击[12−14], 即一旦两块用于加密的相位板被公开之后, 攻击者利用迭代恢复算法就可以恢复得到明文. Abuturab[15−17]提出将这种非对称加密技术应用到gyrator变换域来提高安全性, gyrator变换的变换角度作为密钥增大了系统的密钥空间. 最近, 研究人员提出了基于相位恢复算法的非对称加密系统[18,19], 这种加密系统可以抵抗特殊攻击, 但是由于需要多次迭代, 因此计算量大. 另外, 矢量分解[20]、对数运算[21]以及对数极坐标变化[22]等也被运用到加密系统中实现一些线性变换域的线性移除, 以此来提高加密系统的安全性. 其中, 矢量分解可以不经迭代操作将待加密图像加密为一个唯相位掩膜, 且待加密图像和唯相位掩膜之间满足非线性关系.

除了线性特点, 目前大多数加密算法的加密结果都为复值, 不利于密文的传输和存储, 且需要利用全息技术等干涉方法记录密文的相位来实现解密.

本文利用矢量分解以及gyrator变换的数学实现推导得到了一种新的非对称图像加密方法. 待加密图像先通过矢量分解被加密成两块纯相位板, 其中一块相位板作为解密密钥, 另一块相位板经一系

* 国家自然科学基金(批准号: 61377003)、南京师范大学高层次人才科研启动项目(批准号: 184080H20162)、南京师范大学青年领军人才培养项目(批准号: 184080H20178)和江苏省高校自然科学研究重大项目(批准号: 14KJA140001)资助的课题.

† 通信作者. E-mail: optyuan@163.com

列变换后, 得到实值密文. 本文所设计算法的显著特点是解密密钥不同于加密密钥, 不需要进行迭代即可实现非对称加密, 并且还为实现实值加密提供了一种新的解决方案. 模拟实验验证了此方法的可行性以及安全性.

2 非对称图像加密及解密原理

对一幅待加密的灰度图像 f 进行灰度值归一化处理和矢量分解[20], 获得两个相位分布矩阵 M_1 和 M_2, 可表示为

$$f = |\exp(\mathrm{i}\phi) + \exp[\mathrm{i}(\phi+\varphi)]|^2, \tag{1}$$

$$M_1 = \exp(\mathrm{i}\phi), M_2 = \exp[\mathrm{i}(\phi+\varphi)], \tag{2}$$

其中, ϕ 代表在 $[0, 2\pi]$ 上均匀分布的随机矩阵; φ 与待加密图像 f 有关, 表示为

$$\varphi = \pi - \arccos\left(1 - \frac{f}{2}\right). \tag{3}$$

矢量分解后的 M_1 作为解密密钥. 利用变换角度为 α 的 gyrator 变换对 M_2 进行处理, 可定义为[23]

$$\begin{aligned} &R^{\alpha}[M_2(x,y)] \\ &= \frac{1}{|\sin\alpha|}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} M_2(x,y) \\ &\quad\times \exp\left[\mathrm{i}2\pi\frac{(uv+xy)\cos\alpha-(uy+vx)}{\sin\alpha}\right]\mathrm{d}x\,\mathrm{d}y, \end{aligned} \tag{4}$$

其中 $(x,\ y)$ 和 $(u,\ v)$ 分别为空域坐标和 gyrator 域坐标, $R^{\alpha}[\cdot]$ 表示 gyrator 变换. 其逆变换即进行变换角度为 $-\alpha$ 的 gyrator 变换.

在数学上, gyrator 变换可以用傅里叶变换实现, 表示为[24]

$$\begin{aligned} G(u,v) &= R^{\alpha}[M_2(x,y)] = [(M_2 p) * h]p \\ &= \{\mathrm{IFT}[\mathrm{FT}(M_2 p)\times \mathrm{FT}(h)]\}p, \end{aligned} \tag{5}$$

其中 $*$ 表示卷积运算; FT, IFT 分别表示傅里叶变换和傅里叶逆变换;

$$p = \exp\left(-\mathrm{i}2\pi uv\tan\frac{\alpha}{2}\right), \tag{6}$$

$$h = \frac{1}{|\sin\alpha|}\exp\left(\mathrm{i}\frac{2\pi uv}{\sin\alpha}\right). \tag{7}$$

将 (5) 式两边同时乘以 p^*, 并且进行傅里叶变换, 可以得到

$$\mathrm{FT}(Gp^*) = \mathrm{FT}(M_2 p)H, \tag{8}$$

其中, $H = \mathrm{FT}(h) = \exp(-\mathrm{i}2\pi uv\sin\alpha)$, p^* 表示取 (6) 式 p 的共轭. 因为 H 的模为 1, 所以对 (8) 式两边取模可以得到

$$|\mathrm{FT}(Gp^*)| = |\mathrm{FT}(M_2 p)|, \tag{9}$$

其中 $|\cdot|$ 表示取模.

假设:

$$e = |\mathrm{FT}(Gp^*)|, \tag{10}$$

$$\theta = \mathrm{angle}[\mathrm{FT}(M_2 p)], \tag{11}$$

其中 angle$\{\cdot\}$ 表示取幅角, 则

$$\begin{aligned} &\mathrm{IFT}[e\exp(\mathrm{i}\theta)]p^* \\ &= \mathrm{IFT}[|\mathrm{FT}(Gp^*)|\exp(\mathrm{i}\theta)]p^* \\ &= \mathrm{IFT}[|\mathrm{FT}(M_2 p)|\exp(\mathrm{i}\{\mathrm{angle}[\mathrm{FT}(M_2 p)]\})]p^* \\ &= \mathrm{IFT}[\mathrm{FT}(M_2 p)]p^* \\ &= M_2, \end{aligned} \tag{12}$$

即待加密图像 M_2 经过 gyrator 变换、相位 p^* 调制、傅里叶变换后, 取模得到实值密文 e, 在已知解密密钥 θ 的情况下, 可以通过 (12) 式恢复 M_2, 再利用密钥 M_1 以及 (1) 和 (2) 式即可恢复得到原图像 f, 即

$$f = |M_1 + M_2|^2. \tag{13}$$

根据上面的分析, 我们设计的加密和解密过程的流程如图 1 所示. 加密过程如图 1 (a) 所示: 原图 $f(x,y)$ 经矢量分解被加密到两块相位板 M_1 和 M_2 中, M_1 作为解密密钥, M_2 经过 gyrator 变换, 相位 p^* 调制后再经傅里叶变换, 取模得到实值密文 e. 解密过程如图 1 (b) 所示: 解密过程简单易行, 在解密过程中不需要进行加密过程的 gyrator 变换的逆变换, 且解密密钥不同于加密密钥. 另外, 从 (11) 式可以得到加密过程中产生的解密密钥 θ 是与原图

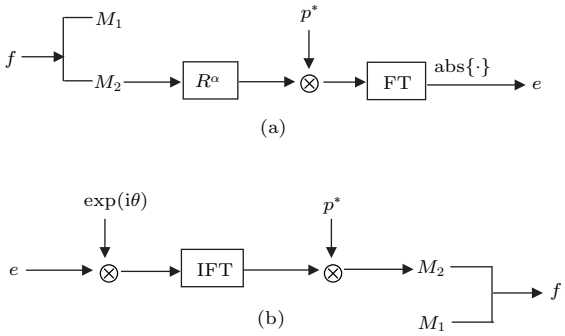


图 1 非对称图像加密流程图 (a) 加密; (b) 解密

Fig. 1. Flowcharts of asymmetric (a) encryption and (b) decryption algorithms.

像直接相关的, 即不同的原图像, 解密密钥θ是不一样的.

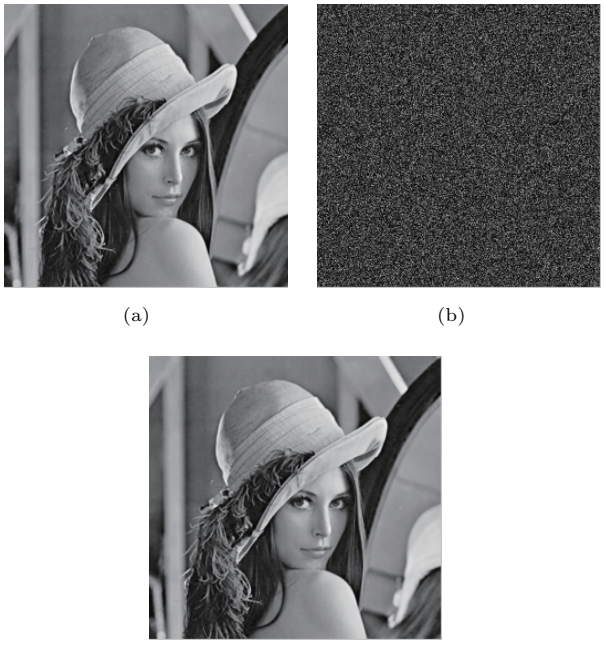
综上所述, 加密过程中gyrator变换的变换角度α以及相位p^*作为加密密钥(公钥), 而相位M_1以及θ作为解密密钥(私钥), 解密密钥不同于加密密钥, 实现了非对称加密, 增大了加密系统的安全性.

3 实验结果与安全性分析

在计算机模拟实验中, 待加密的图像如图2(a)所示, 像素大小为256×256, gyrator变换的变换角度α为0.4π, 加密结果如图2(b)所示. 我们用相关系数(CC)来评估解密图像的质量, 其中$f(x,y)$代表原始图像, $\tilde{f}(x,y)$代表解密后的图像, $E(\cdot)$代表期望.

$$CC=\frac{E\{(f-E(f))(\tilde{f}-E(\tilde{f}))\}}{\sqrt{E\{(f-E(f))^2\}}\sqrt{E\{(\tilde{f}-E(\tilde{f}))^2\}}}. \tag{14}$$

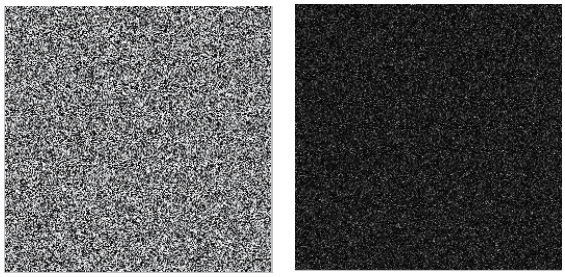
正确的解密图如图2(c)所示, 其与原图像之间的相关系数值为1. 解密时, 密钥M_1以及θ错误时的解密结果如图3(a)和图3(b)所示, 相关系数值分别为0.0014, 0.0025. 因此, 当任何一个解密密钥错误时, 都无法从解密图得到原图的任何信息.



(a) (b) (c)

图2 加密算法模拟结果 (a) 原图; (b) 密文; (c) 解密图

Fig. 2. (a) Original image Lena, (b) ciphertext, and (c) the decrypted image.



(a) (b)

图3 密钥错误的解密图 (a) M_1错误; (b) θ错误

Fig. 3. Decrypted images with (a) incorrect key M_1, and (b) incorrect key θ.

3.1 密钥的敏感性分析

为了验证私钥θ的灵敏度, 假设私钥θ在受到干扰时, 其值会在一定范围内浮动, θ'与θ之间的差距非常小, 可以表示为

$$\theta'=\theta+d\Delta\theta, \tag{15}$$

其中$\Delta\theta$为值分布在$(-2\pi,2\pi)$之间的随机矩阵, d为系数, 其值分布在$(-1,1)$. 图4给出了相关系数值随d变化的曲线图以及d分别等于0.1和0.2时的解密图, 可以看到当d为0.2时, 原图的具体信息已经无法识别. 因此, 加密系统对密钥θ的敏感性很高, 能够抵抗暴力攻击.

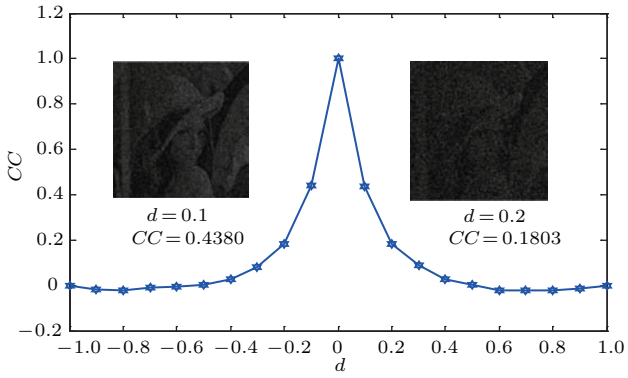


图4 相关系数CC随d变化的曲线图以及$d=0.1$, 0.2时的解密图

Fig. 4. The CC for the perturbation of the decryption key θ including decrypted images obtained with $d=0.1$, 0.2.

3.2 抗噪声和抗剪切攻击分析

我们给图2(b)密文模拟添加了均值为0 方差为1的高斯随机噪声N, 噪声干扰密文的方式为

$$e'=e(1+kN), \tag{16}$$

其中, e 和 e' 分别为原始密文和受到噪声干扰后的密文, k 为噪声强度系数. 图5给出了相关系数值随噪声强度系数 k 变化的曲线图以及当噪声强度 k 为0.2和0.6时得到的解密图, 可以看到, 当噪声强度为0.6时, 仍可辨别出原始图像的轮廓, 因此该加密系统具有一定的抗噪声攻击能力.

为了测试加密系统的抗剪切能力, 我们将图2 (b) 密文的某些像素值置0, 从图6的模拟结果图可以看到, 当密文信息丢失25%, 解密得到的图像仍可看到明文的主要特征, 说明加密系统有较高抗剪切能力.

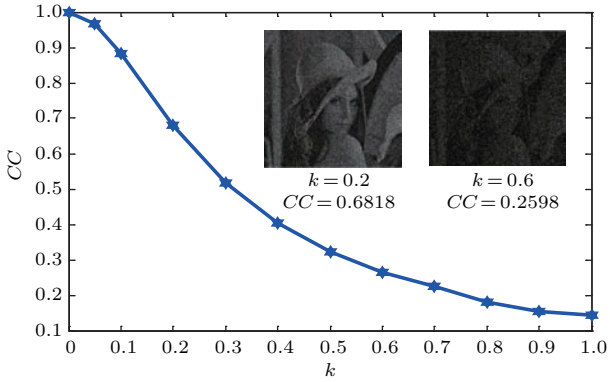


图5 相关系数 CC 随 k 变化的曲线图以及 $k = 0.2$, 0.6 时的解密图

Fig. 5. The CC curve of noise attack including decrypted images obtained with $k = 0.2$, 0.6.

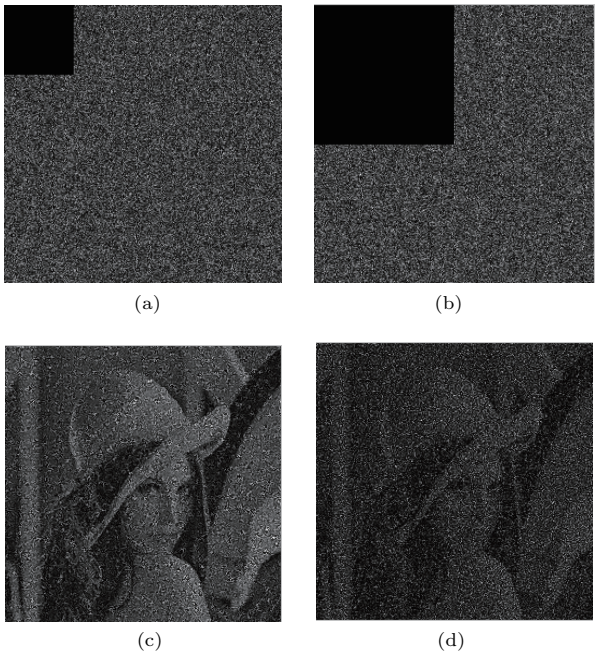


图6 剪切攻击模拟结果图 (a) 信息丢失6.25%的密文图; (b) 信息丢失25%的密文图; (c) 密文信息丢失6.25%的解密图; (d) 密文信息丢失25%的解密图

Fig. 6. Ciphertext with (a) 6.25% occlusion, (b) 25% occlusion; (c) decrypted image from (a); (d) decrypted image from (b).

3.3 抗选择明文攻击分析

通常情况下, 针对加密系统的攻击主要有已知明文攻击、选择明文攻击、选择密文攻击、唯密文攻击. 由于选择明文攻击对加密系统最有威胁, 如果加密系统能够抵抗选择明文攻击, 则可以抵抗另外三种攻击[25]. 因此, 在本文中, 我们用选择明文攻击来进一步测试系统的安全性. 对于选择明文攻击, 攻击者已经知道加密和解密算法, 并且可以任意选择明文, 并利用公钥获取相应的密文. 假设攻击者通过加密如图7 (a) 所示图像, 获取了解密密钥 M_1' 以及 θ', 并利用它们解密如图2 (b) 所示密文, 解密结果如图7 (b) 所示, 可以看到无法从解密图得到原图Lena的任何信息. 这是由于算法的相位密钥即私钥的产生与被加密信息密切相关, 即不同的明文对应不同的解密私钥, 攻击者不可能通过其他明文密文对来攻击系统获得解密原始明文的私钥, 从而获取原始明文. 因此, 算法能够抵抗选择明文攻击.

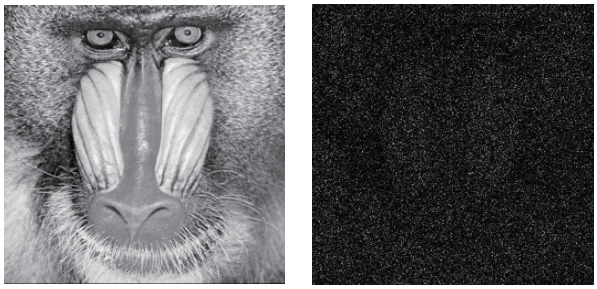


图7 选择明文攻击模拟结果 (a) 伪明文Baboon; (b) 解密图Lena

Fig. 7. Results of chosen plaintext attack: (a) The fake plaintext Baboon; (b) decrypted image Lena.

4 结 论

本文利用矢量分解以及gyrator变换的数学实现获得了一种新的非对称图像加密方法. 待加密图像先通过矢量分解被加密成两块纯相位板, 其中一块相位板作为解密密钥, 另一块相位板经过gyrator变换、相位 p^* 调制、傅里叶变换后, 得到最终的实值密文. 加密过程中产生的两个相位密钥作为私钥, 私钥与公钥的不同使攻击者无法用加密密钥完成解密, 且相位密钥的产生与被加密信息密切相关, 使系统能有效抵抗各类已知的基于明文密文对的攻击. 模拟实验证明了算法能够抵抗暴力攻击、噪声攻击、剪切攻击和选择明文攻击.

参考文献

[1] Refregier P, Javidi B 1995 *Opt. Lett.* **20** 767
[2] Deng X P, Zhao D M 2012 *Opt. Lasers Technol.* **44** 136
[3] Abuturab M R 2015 *Opt. Lasers Eng.* **69** 49
[4] Liu Z J, Guo C, Tan J B, Liu W, Wu J J, Wu Q, Pan L Q, Liu S T 2015 *Opt. Lasers Eng.* **68** 87
[5] Sui L S, Xin M T, Tian A L, Jin H Y 2013 *Opt. Lasers Eng.* **51** 1297
[6] Chen W, Chen X 2012 *Appl. Opt.* **51** 6076
[7] Rajput S K, Nishchal N K 2013 *Appl. Opt.* **52** 4343
[8] Peng X, Zhang P, Wei H Z, Yu B 2006 *Acta Phys. Sin.* **55** 1130 (in Chinese) [彭翔, 张鹏, 位恒政, 于斌 2006 物理学报 **55** 1130]
[9] Peng X, Wei H Z, Zhang P 2007 *Acta Phys. Sin.* **56** 3924 (in Chinese) [彭翔, 位恒政, 张鹏 2007 物理学报 **56** 3924]
[10] Frauel Y, Castro A, Naughton T J, Javidid B 2007 *Opt. Express* **15** 10253
[11] Qin W, Peng X 2010 *Opt. Lett.* **35** 118
[12] Rajput S K, Nishchal N K 2012 *Appl. Opt.* **51** 5377
[13] Rajput S K, Nishchal N K 2014 *J. Opt. Soc. Am. A* **31** 1233
[14] Mehra I, Nishchal N K 2015 *Opt. Commun.* **354** 344
[15] Abuturab M R 2014 *Opt. Lasers Eng.* **58** 39
[16] Abuturab M R 2014 *Opt. Commun.* **323** 100
[17] Abuturab M R 2015 *Opt. Lasers Eng.* **69** 49
[18] Rajput S K, Nishchal N K 2014 *Appl. Opt.* **53** 418
[19] Wang Y, Quan C, Tay C J 2016 *Opt. Lasers Eng.* **78** 8
[20] Wang X G, Zhao D M 2011 *Opt. Commun.* **284** 945
[21] Joshi M, Shakher C, Singh K 2009 *Opt. Lasers Eng.* **47** 721
[22] Zhou N R, Wang Y X, Gong L H 2011 *Opt. Commun.* **284** 3234
[23] Rodrigo J A, Alieva T, Calvo M L 2007 *Opt. Express* **15** 2190
[24] Liu Z, Chen D, Ma J, Wei S, Zhang Y, Dai J 2011 *Optik* **122** 864
[25] Zhang Y, Xiao D 2013 *Opt. Lasers Eng.* **51** 472

Asymmetric image encryption method based on gyrator transform and vector operation*

Yao Li-Li Yuan Cao-Jin† Qiang Jun-Jie Feng Shao-Tong Nie Shou-Ping

(*Key Laboratory for Opto-Electronic Technology of Jiangsu Province, Nanjing Normal University, Nanjing 210023, China*)

(Received 15 June 2016; revised manuscript received 6 July 2016)

Abstract

With the rapid development of computer network technology, information security has attracted increasing attention. Due to the characteristics of multi-dimensional operation and parallel processing capability, optical image encryption techniques have been receiving more and more attention. Since the well-known double random phase encoding technique was proposed, many other methods based on optical information processing means such as the use of optical transform, interference, and polarized light encoding, have been proposed for optical image encryption. However, recent researches have demonstrated that traditional optical encryption techniques are symmetric cryptosystems, in which decryption keys are identical to encryption keys and they have been found to be vulnerable to different types of attacks, such as known plaintext and chosen plaintext attacks. To overcome this shortcoming, asymmetric cryptosystems based on nonlinear phase-truncation techniques and phase retrieval algorithm have been proposed. Asymmetric cryptosystem is a cryptographic system in which encryption keys are different from decryption keys. The encryption keys are used as public keys which are disseminated widely, and the decryption keys are used as private keys which are known only to the authorized users. So, asymmetric cryptosystem can offer a higher-level security than symmetric cryptosystem. However, asymmetric cryptosystems based on phase retrieval algorithms require a lot of computational time, and asymmetric cryptosystems based on phase-truncated Fourier transforms have been found to be vulnerable to special attack. Therefore, in this paper, a novel asymmetric image encryption method is proposed by using the gyrator transform and vector operation. The original image is encrypted into two phase masks with vector operation. One is a random phase mask and the other is a phase mask related to the original image. In the encryption process, the random phase mask is used as a phase key and the other phase mask is transformed by gyrator transform. The transform result is performed by Fourier transform after being modulated by a phase distribution. The ciphertext is the amplitude of the above result. Compared with previous encryption schemes, the suggested method has two advantages. Firstly, we have proposed a new asymmetric encryption method based on the gyrator transform and vector operation. The decryption process is different from the encryption process. The gyrator transform and Fourier transform are used in the encryption process, while only the inverse operation of Fourier transform is employed in the decryption process. In addition, the decryption keys produced in the encryption process are different from the encryption keys. Therefore, the proposed scheme has high resistance against the conventional attacks. Secondly, the encrypted result is real-valued, which is convenient for display, transmission and storage. Numerical simulations illustrate the feasibility and effectiveness of the proposed encryption scheme.

Keywords: gyrator transform, asymmetric encryption, vector operation, real-valued encryption

PACS: 42.30.–d, 42.30.Kq, 42.30.Va **DOI:** 10.7498/aps.65.214203

* Project supported by the National Natural Science Foundation of China (Grant No. 61377003), the Scientific Research Foundation for Advanced Talents, Nanjing Normal University, China (Grant No. 184080H20162), the Training Program Foundation for Youth Leader Talents by Nanjing Normal University, China (Grant No. 184080H20178), and the Major Natural Science Research Project for Universities of Jiangsu Province, China (Grant No. 14KJA140001).

† Corresponding author. E-mail: optyuan@163.com