基于改进后多维数据加密系统的多图像光学加密算法的研究*

徐宁[1)] 陈雪莲[1)] 杨庚[2)]

1) (南京邮电大学光电工程学院, 南京 210046)

2) (南京邮电大学计算机学院, 南京 210046)

(2012年8月14日收到; 2012年11月2日收到修改稿)

提出了以改进后的基于虚拟成像的多维数据加密系统 (VOI) 为基础的多图像加密算法. 首先构造多幅图像横向叠加作为加密对象, 结合改进后的 VOI 系统完成加密. 对 VOI 系统做了三方面改进: 加密图像编码为相位信息, 提高了图像的可分辨性和系统的解密效果; 随机相位板与随机振幅板结合, 提升了系统的密钥空间和对抗暴力攻击的能力; 像平面前增添随机相位板, 增强了系统的安全性. 采用峰值信噪比评价算法加密效果, 计算结果表明本算法与原算法相比具有更好的有效性、鲁棒性和安全性.

关键词: 多维数据加密系统, 虚拟光学, 相位编码, 峰值信噪比

PACS: 42.30.−d **DOI:** 10.7498/aps.62.084202

1 引 言

基于光学理论与方法的数据加密是光学信息安全领域中一个较为活跃的研究方向 [1−8]. 近年来, 光学加密技术不仅针对单幅图像的加密, 多图像加密也成为研究热点. 它在多用户认证、内容分发、提高秘密信息传输效率等方面具有很高的应用价值. 主要方法包括位相抽取 [9]、数字全息术、波长复用 [10]、扩频技术 [11]、计算全息和联合迭代相位恢复等. 然而, 现有方法大多采用多幅加密图像经编码后实施的纵向迭加操作, 其所产生的加性串扰造成提取图像质量明显下降, 复用容量被严重限制. 为此, 本文提出基于横向叠加多图像加密算法, 并结合改进后的多维数据加密系统 (VOI) 光学加密系统完成多幅图像加密. 由于多幅图像为横向叠加, 避免了纵向叠加所产生的加性串扰, 提高了解密图像的像质.

2 算法描述

2.1 加密算法

本文提出的多图像加密由两部分组成, 加密图像采用目前市场上普遍使用的标准二维码图像, 读取传输均可通过手机, 使用方便, 具有实用价值. 第一部分通过计算机完成四幅二维码图像的横向叠加, 该部分的物理模型如图 1 所示. $f_1(x_1,y_1)$; $f_2(x_2,y_2)$; $f_2(x_2,y_2)$; $f_4(x_4,y_4)$ 分别表示待加密的四幅二维码图像, 经编码横向叠加的二维码图像由 $f(x,y)$ 表示. 从图 1 中可以看出, f 包含了原 f_1, f_2, f_3, f_4 的所有信息, 其过程如 (1) 式

$$f(x,y)=\mathrm{SUM}\{f_1(x_1,y_1);f_2(x_2,y_2);f_3(x_3,y_3);f_4(x_4,y_4)\}. \quad (1)$$

第二部分为改进后的 VOI 系统. 加密系统如图 2 所示, 信息平面处放置横向叠加图像 $f(x,y)$, 将其

* 国家重点基础研究发展计划 (批准号: 2011CB302903)、国家自然科学基金 (批准号: 61272084, 61202353)、江苏省自然科学基金 (批准号: BK2009426) 和江苏省高校自然科学研究重大项目 (批准号: 11KJA520002) 资助的课题.

† 通讯作者. E-mail: chenxuelian1988@126.com; xuning@njupt.edu.cn

© 2013 中国物理学会 Chinese Physical Society

相位编码后得到图像用 $F(x,y)$ 表示, 随机生成相位模板为 $R_1(x,y)$, 随机振幅模板 $R_2(x,y)$, 对 $R_1(x,y)$ 进行振幅调制, 生成随机模板信息 $R(x,y)$. 算法表示如下:

$$F(x,y)=\exp\{\mathrm{j}\cdot f(x,y)\}, \tag{2}$$

$$R(x,y)=R_1(x,y)\times R_2(x,y). \tag{3}$$

根据傅里叶光学, 波长为 λ 的虚拟光波从物平面到透镜前表面和虚拟光波从透镜后表面到像平面的传播过程可用菲涅尔衍射变换描述. 因此, 从图 2 可以看出, $F(x,y)$ 经过衍射距离为 d_0 的菲涅尔衍射变换后, 在透镜前表面生成 $N_1(x,y)$; $R(x,y)$ 经过衍射距离为 (d_1+d_2) 的菲涅尔变换后, 在透镜前表面生成 $N_2(x,y)$; 通过 $N_1(x,y)$ 和 $N_2(x,y)$ 在透镜处的非相干叠加, 得到 $N(x,y)$, $N(x,y)$ 通过透射率为 $t(x,y;f)$ 的透镜, 经距离为 d_i 的衍射, 再由随机相位板 $R_3(x,y)$ 的相位调制, 在像平面处得到密文 $U(x,y)$. 若 $\mathrm{FrT}_{\lambda,d_0}\{\ \}$ 表示波长为 λ, 衍射距离为 d_0 的菲涅尔衍射变换, 则上述算法可表示为

$$\begin{aligned}N(x,y)=&\mathrm{FrT}_{\lambda,d_0}\{F(x,y)\}\\&+\mathrm{FrT}_{\lambda,d_1+d_2}\{R(x,y)\},\end{aligned} \tag{4}$$

$$\begin{aligned}U(x,y)=&R_3(x,y)\times\mathrm{FrT}_{\lambda,d_i}\{N(x,y)\\&\times t(x,y;f)\}.\end{aligned} \tag{5}$$

2.2 解密算法

解密算法是上述两部分算法的逆过程, 用 $\mathrm{IFrT}_{\lambda,d}\{\cdot\}$ 表示菲涅尔逆变换, 首先对随机相位板 $R_3(x,y)$ 和透镜做逆变换, 得到透镜前表面的叠加信息 $\mathrm{De}N(x,y)$ 过程如下:

$$\mathrm{De}U(x,y)=U(x,y)/R_3(x,y), \tag{6}$$

$$\mathrm{De}N(x,y)=\mathrm{IFrT}_{\lambda,d_i}\{\mathrm{De}U(x,y)/t(x,y;f)\}; \tag{7}$$

再减去 $R(x,y)$ 在透镜前表面形成的菲涅尔衍射影响, 得到信息平面 $F(x,y)$ 在透镜前表面形成的菲涅尔衍射 $\mathrm{De}N_1(x,y)$:

$$\begin{aligned}\mathrm{De}N_1(x,y)=&\mathrm{De}N(x,y)-\mathrm{FrT}_{\lambda,d_1+d_2}\{R_1(x,y)\\&\times R_2(x,y)\};\end{aligned} \tag{8}$$

再经过菲涅尔逆变换和相位编码的逆变换, 得到信息平面 $f(x,y)$ 的解密结果:

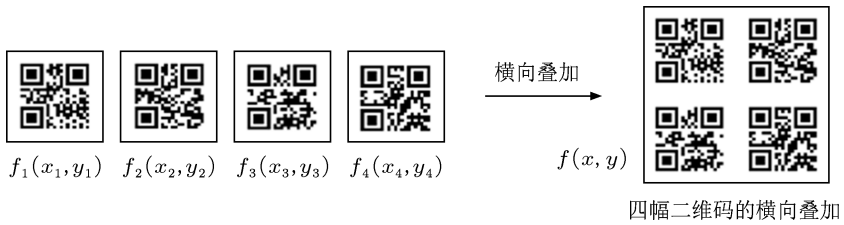


图 1 四幅二维码横向叠加

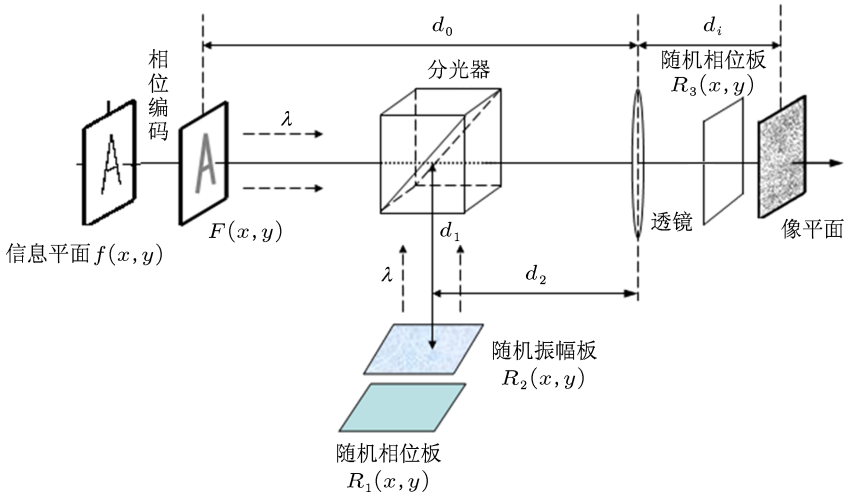


图 2 改进后的 VOI 加密系统结构图

$$\mathrm{De}F(x,y)=\mathrm{IFrT}_{d_0}\{\mathrm{De}N_1(x,y)\},\tag{9}$$

$$\mathrm{De}f(x,y)=\arccos\{\mathrm{Re}\{\mathrm{De}F(x,y)\}\};\tag{10}$$

最终将得到信息分割成原来的四幅二维码, 表示如下:

$$\mathrm{De}f_1(x_1,y_1)=\mathrm{DeSUM}_{11}\{\mathrm{De}f(x,y)\},\tag{11}$$

$$\mathrm{De}f_2(x_2,y_2)=\mathrm{DeSUM}_{12}\{\mathrm{De}f(x,y)\},\tag{12}$$

$$\mathrm{De}f_3(x_3,y_3)=\mathrm{DeSUM}_{21}\{\mathrm{De}f(x,y)\},\tag{13}$$

$$\mathrm{De}f_4(x_4,y_4)=\mathrm{DeSUM}_{22}\{\mathrm{De}f(x,y)\}.\tag{14}$$

2.3 基于峰值信噪比的评价方法

本文采用峰值信噪比 (PSNR) 进行解密图像的质量评价, 以判定系统的加密解密效果. 计算方法为

$$\mathrm{MSE}=\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(f_{ij}-\mathrm{De}f_{ij})^2,\tag{15}$$

$$\mathrm{PSNR}=10\log_{10}\frac{L^2}{\mathrm{MSE}},\tag{16}$$

其中 MSE 为均方误差, 是加密与解密图像之间总的灰度差, 可以理解为噪声信号; PSNR 是峰值信号与噪声的比值, 比值越大, 两幅图像相似度越高, 当高于 35—40 时, 肉眼分辨不出差异; N 和 M 是图像矩阵维度数, L 是图像最大灰度值. 通常 8 bit 的图像 L 为 255, 若图像矩阵像素点的灰度值类型是 1 或 0, 则 L 为 1.

改进后 VOI 系统除原系统的密钥 $\{\lambda,d_0,d_1,d_2\}$ 外, 增加了随机振幅板 $R_2(x,y)$ 和随机相位板 $R_3(x,y)$, 增大了系统的密钥空间的维数, 增强了系统抵抗暴力攻击的能力, 提高了系统的安全性.

3 计算模拟与分析

3.1 加密解密算法正确性分析

本文采用 matlab 仿真, 加密对象如图 1 所示 $f(x,y)$, 波长取值为 632.8 nm, 每幅图像有效采点数为 116×116, 衍射距离 $\{d_0,d_1,d_2\}$ 分别取为 $\{10,20,10\}$ mm.

叠加图像相位编码 $F(x,y)$ 如图 3(a) 所示, 密文 $U(x,y)$ 如图 3(b) 所示, 相位编码解密 $\mathrm{De}F(x,y)$ 如图 3(c) 所示, 叠加图像解密 $\mathrm{De}f(x,y)$ 如图 3(d) 所示, 解密图像 $\mathrm{De}f_1(x_1,y_1)$, $\mathrm{De}f_2(x_2,y_2)$, $\mathrm{De}f_3(x_3,y_3)$, $\mathrm{De}f_4(x_4,y_4)$ 分别如图 4(e)—(h) 所示.

如图 3 所示, 四幅解密图像的 PSNR 分别为 156.0728, 155.8671, 156.0261 和 155.7347, 因此, 解密图像与原图基本一致, 表明了本加密系统的有效性.

3.2 安全性分析

在改进方法一中, 通过在随机相位板 $R_1(x,y)$ 中叠加随机振幅板 $R_2(x,y)$, 提高了系统的安全性. 事实上, 对原 VOI 系统, 当攻击者已知密文 $U(x,y)$ 和除了随机相位板 $R_1(x,y)$ 外所有密钥 $\{\lambda,d_0,d_1,d_2\}$ 时, 采用任意随机相位模板 $R_1'(x,y)$ 解密, 解密结果如图 4(a) 所示, 原图信息基本还原,

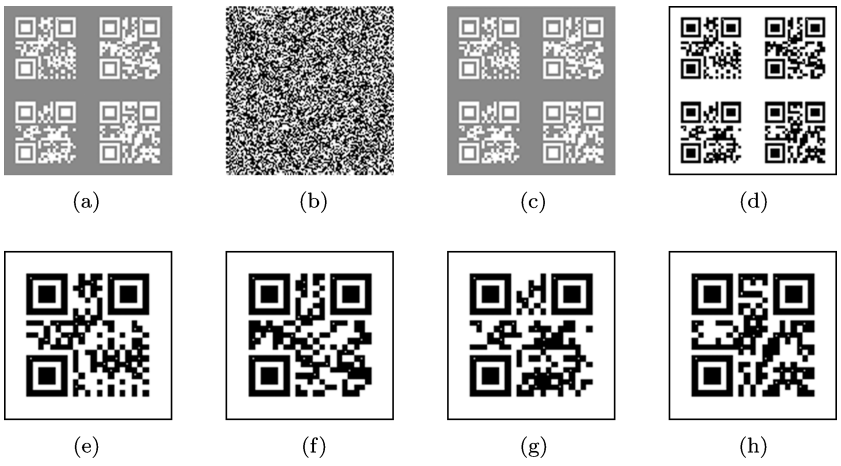


图 3 (a) $F(x,y)$; (b) $U(x,y)$; (c) $\mathrm{De}F(x,y)$; (d) $\mathrm{De}f(x,y)$; (e) $\mathrm{De}f_1(x_1,y_1)$; (f) $\mathrm{De}f_2(x_2,y_2)$; (g) $\mathrm{De}f_3(x_3,y_3)$; (h) $\mathrm{De}f_4(x_4,y_4)$

且解密图像的 PSNR 值为 14.04; 但在改进后的 VOI 系统中仅添加了随机振幅板 $R_2(x,y)$, 针对上述情况, 解密结果如图 4(b), 解密图像 PSNR 值为 7.01. 若攻击者已知随机振幅板和随机相位板的叠加方法, 同时生成两个随机板 $R_1'(x,y)$ 和 $R_2'(x,y)$ 解密, 其结果如图 4(c), PSNR 值为 7.05. 综上所述, 攻击者已知密钥和密文, 未知随机信息, 原 VOI 系统的解密结果含有原图的大部分信息, 改进后的 VOI 系统解密图像基本是噪声, 比较前后两系统 PSNR 值, 改进后的 VOI 系统安全性有所提高.

在改进方法二中, 通过添加随机相位板 $R_3(x,y)$, 提高了系统的安全性. 事实上, 若攻击者已知原 VOI 系统的所有密钥 $\{\lambda, d_0, d_1, d_2, R_1(x,y)\}$ 和密文 $U(x,y)$, 未知随机相位板 $R_3(x,y)$ 直接进行解密, 解密结果如图 4(d) 所示, PSNR 值为 2.08; 若已知加入 $R_3(x,y)$, 产生任意随机相位板 $R_3'(x,y)$ 解密, 结果如图 4(e) 所示, PSNR 为负值.

上述分析讨论表明, 原 VOI 系统对抗暴力攻击的能力弱, 在随机相位板未知的情况下, 攻击者可以还原被加密的原始图像信息, 达到窃取图像信息的目的, 破坏了信息的机密性. 而改进后的 VOI 系统能够抵抗暴力攻击, 提高了系统的安全性.

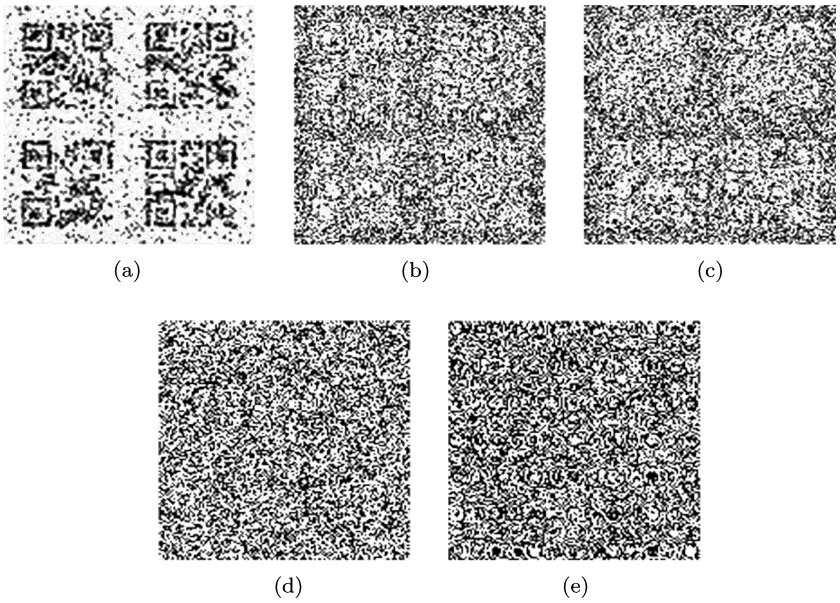


图 4 (a) 原 VOI 中, 任意 $R_1'(x,y)$ 解密结果; (b) 改进的 VOI 中, 任意 $R_1'(x,y)$ 解密结果; (c) 改进的 VOI 中, 任意 $R_1'(x,y)$ 和 $R_2'(x,y)$ 的解密结果; (d) 改进的 VOI 中, 任意 $R_3(x,y)$ 解密结果; (e) 改进的 VOI 中, 任意 $R_3'(x,y)$ 解密结果

4 算法分析

作为面向数据加密应用的算法, 其鲁棒性和安全性是算法的重要特征. 本节分析改进后的 VOI 系统对抗各类噪声以及密钥失真时所表现的性质.

首先分析算法对抗各类噪声的鲁棒性. 本文模拟了高斯噪声、泊松噪声、椒盐噪声等对算法的影响. 相比较三种噪声, 因算法对高斯噪声效果相对较差, 选择高斯噪声作为分析对象, 均值和方差取值分别为 0, 0.01. 图 5 为高斯噪声加到密文上时的解密结果. 四个二维码解密结果的 PSNR 为 64.2307, 75.7968, 60.5291, 66.2979. 可以看出, 信息丢失少, 解密效果好, 因此本算法对抗各类噪声的能力强.

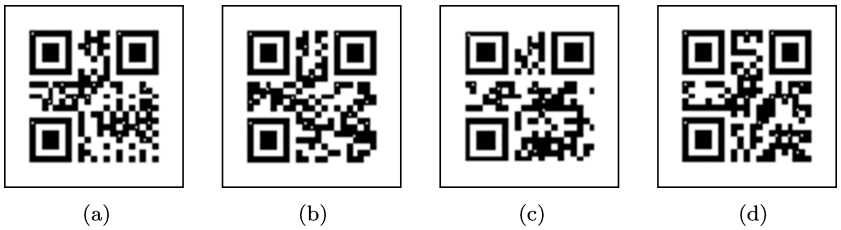
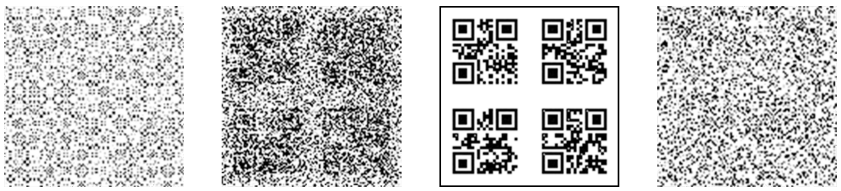


图 5 高斯噪声影响情况下的解密结果 (a) $\mathrm{De}f_1(x_1,y_1)$; (b) $\mathrm{De}f_2(x_2,y_2)$; (c) $\mathrm{De}f_3(x_3,y_3)$; (d) $\mathrm{De}f_4(x_4,y_4)$

下面分析在密钥失真情况下系统的安全性. 首先分析系统原有的四个密钥 $\{d_0,d_1,d_2,\lambda\}$ 对安全性的影响, 然后讨论增加的密钥对 $\{R_2(x,y),R_3(x,y)\}$ 对安全性的影响.

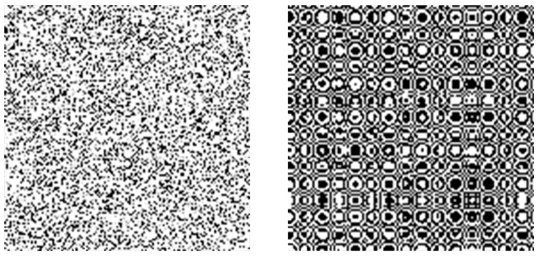
图 6(a), (b), (c) 显示了将密钥中的衍射距离 $\{d_0,d_1,d_2\}$ 改变 0.3, 0.4 和 0.5 mm 时 (假设其余密钥都正确), 分别解密出的 De$F(x,y)$; 图 4(d) 则显示了密钥 λ 发生变化时, 解密出的 De$F(x,y)$. 当 d_0 改变 0.3 mm 时, 图像解密的质量比较差, 原图像的特征已经被丢失, 解密图像的 PSNR 只有 3.8517, 这表明本文提出的加解密算法对密钥 d_0 是不敏感的, 该密钥可以起到增强算法安全的作用; 但是当 d_1 改变 0.4 mm 时, 解密出的结果能大致看出有四幅二维码, 显示了原始图像的轮廓, 泄露了少许信息, 此时 PSNR 为 7.0428; 而当 d_2 改变 0.5 mm 时, 解密出的结果非常清晰, PSNR 甚至达到 49.6170, 原图信息完全泄露, 表明加解密算法对该密钥敏感, 密钥的微小变化就可以得到原始图像的部分信息, 破坏了算法的机密性. 当解密密钥 λ 取 500×10^{-5} m 时, 解密结果同样也是很差的, PSNR 只有 6.7680.



(a) (b) (c) (d)

图 6 (a) 密钥 d_0 失真时候的解密结果; (b) 密钥 d_1 失真时的解密结果; (c) 密钥 d_2 失真时的解密结果; (d) 密钥 λ 失真时的解密结果

从上述分析中可知, 系统密钥 $\{d_0,d_1,d_2,\lambda\}$ 中, 加解密算法对 d_0 和 λ 不敏感, 这两个密钥的微小变化解不出加密的图像信息. 反之, 密钥 d_2 对系统几乎没有什么保护性, 攻击者在不需要知道它的情况下, 可以解密出较清晰的原始图像. 因此原 VOI 系统的密钥安全性不够强, 而本文希望通过增加两个随机模板作为新密钥来增强系统的安全性. 下面讨论其对算法安全性的影响.



(a) (b)

图 7 (a) 密钥 $R_2(x,y)$ 失真时的解密结果; (b) 密钥 $R_3(x,y)$ 失真时的解密结果

当随机振幅板 $R_2(x,y)$ 失真时, 解密结果如图 7(a) 所示, PSNR 值只有 5.9134; 当随机相位板 $R_3(x,y)$ 失真时, 解密结果如图 7(b) 所示, PSNR 是负值. 从解密图像可以看出, 当附加密钥 $\{R_2(x,y),R_3(x,y)\}$ 失真时, 解密质量非常差, 几乎看不出任何原图信息.

因此, 可以看出, 在系统的原有密钥 $\{d_0,d_1,d_2,\lambda\}$ 中, d_2 的保护性较差, 无法保证算法的安全性, 通过附加密钥对随机振幅板 $R_2(x,y)$ 和随机相位板 $R_3(x,y)$ 可以弥补该缺陷, 提高了系统的安全性.

5 结 论

本文提出并模拟证实了以改进后的基于虚拟成像的 VOI 为基础的多图像加密算法的有效性、鲁棒性和安全性. 该算法可同时加密多幅图像, 消除了图像间的串扰, 使得解密图像质量得到提高. 同时该算法提高了系统的安全性, 解决了原有 VOI 系统安全性不高的问题. 模拟结果显示该加密算法具有进行多幅图像信息同时加密的性能和可实际应用的潜在价值.

[1] Xiao Y L, Su X Y, Li S K, Liu X Q, Zeng S G 2011 *Opt. Laser Technol.* **43** 889

[2] Wang B, Zhang Y 2009 *Opt. Commum.* **282** 3439

[3] Qin W, Peng X 2010 *Opt. Lett.* **35** 118

[4] Wang X G, Zhao D M 2011 *Appl. Opt.* **50** 6645

[5] Yang H Q, Liao X F, Kwok-Wo Wong 2012 *Acta Phys. Sin.* **61** 040505 (in Chinese) [杨华千, 廖晓峰, Kwok-Wo Wong 2012 物理学报 **61** 040505]

[6] Peng X, Wei H Z, Zhang P 2008 *Optical Information Security Introduction* (Beijing: Science Press) p164 (in Chinese) [彭翔, 位恒政, 张鹏 2008 光学信息安全导论 (北京: 科学出版社) 第 164 页]

[7] Wang J, Jiang G P 2011 *Acta Phys. Sin.* **60** 060503 (in Chinese) [王静, 蒋国平 2011 物理学报 **60** 060503]

[8] Jin J X, Qiu S S 2010 *Acta Phys. Sin.* **59** 792 (in Chinese) [晋建秀, 丘水生 2010 物理学报 **59** 792]

[9] Shi Y S, Wang Y L, Xiao J 2011 *Acta Phys. Sin.* **60** 034202 (in Chinese) [史祎诗, 王雅丽, 肖俊 2011 物理学报 **60** 034202]

[10] Situ G H, Zhang J J 2005 *Opt. Kff.* **30** 1306

[11] Hennelly B M, Naughton T J, Mcdonald J 2007 *Opt. Lett.* **32** 1060

Research on the algorithm of multiple-image encryption based on the improved virtual optical imaging*

Xu Ning[1)] Chen Xue-Lian[1)] Yang Geng[2)]

1) (*College of Opto-Electronic Engineering, Nanjing University of Post and Telecommunications, Nanjing* 210046*, China*)

2) (*College of Computer, Nanjing University of Post and Telecommunications, Nanjing* 210046*, China*)

(Received 14 August 2012; revised manuscript received 2 November 2012)

Abstract

In this paper we propose an algorithm for multiple-image encryption based on the improved virtual optical imaging (VOI). The improved algorithm enhances the security by integrating several images into one as an encrypting object and increasing key space. It focuses on three issues. First, it encrypts the phase information, which can improve the performance of decryption effect of the system. Second, it combines random phase plate with a random amplitude board at the position of the random phase plate to increase the dimension of the key space and the ability to resist the attacks. Finally, it adds a random phase plate before the image place, which enhances the security of the system. It uses the peak signal-to-noise ratio to evaluate the performance of the proposed algorithm. Compared with the traditional VOI-based encryption method, the simulations show that the proposed method demonstrates a good performance in the sense of feasibility, robustness and security.

Keywords: virtual optical imaging, phase coding, peak signal to noise ratio, information security

PACS: 42.30.−d **DOI:** 10.7498/aps.62.084202

* Project supported by the National Basic Research Program of China (Grant No. 2011CB302903), the National Natural Science Foundation of China (Grant Nos. 61272084, 61202353), the Natural Science Foundation of Jiangsu Province, China (Grant No. BK2009426), and the Key University Natural Science Research Project of Jiangsu Province, China (Grant No. 11KJA520002).

† Corresponding author. E-mail: chenxuelian1988@126.com; xuning@njupt.edu.cn