

基于随机相位实值编码的光学图像加密*

李榕 李萍

(华南师范大学物理与电信工程学院, 广州 510631)

摘要 提出了一种用于图像加密的随机相位实值编码方法, 待编码的纯相位图像与一个随机相位掩膜一起作傅里叶变换, 取其实部作为编码图像. 已编码的图像和随机相位掩膜的傅里叶变换相加作傅里叶反变换, 反变换的光强可以准确地重建原图像. 该编译码方法简单, 编码图像是一个实值图像, 便于计算机打印或显示输出.

关键词 光学图像加密; 随机相位编码; 实值编码

中图分类号 TN911 **文献标识码** A

0 引言

光学信息处理具有高速的并行处理能力, 以及能用复数函数处理数据的能力, 因此它在图像加密和光安全方面的应用引起了国内外许多学者的研究兴趣^[1~4]. B. Javidi 等人提出的双随机相位编码技术, 分别在空域和频域用两个随机相位掩膜对原图像编码. 但是用该编码方法编码出的图像是一个复值图像, 在某些应用场合, 特别是光电混合系统中, 如需要将编码后的图像打印或者显示出来时, 只能取其部分信息(光强或相位, 实部或虚部等), 这样重构的原图像会严重失真. 文献[5]提出了一种单随机相位的实值编码方法, 该方法的编码图像是实值, 但是解码的图像已经严重退化. 本文通过对该编码方法分析研究, 提出了一种新的编码解码方法, 不仅编码图像是一个实值图像, 而且用与编码键相同的解码键解码, 可以完全重构原图像.

1 光学图像编码及解码方法

1.1 基本算法

编码和译码的过程可以通过图1所示的光学系统实现. 其中图1(a)是编码过程.

原图像 $f_0(x, y)$ 是一个灰度图像, $f_0(x, y)$ 的取值范围在 $[0, 1]$ 之间. 首先将其转换为纯相位图像 $f(x, y) = \exp[i\pi f_0(x, y)]$, 编码键是一个随机的二值纯相位掩膜, $r(x, y) = \exp[i\pi r_0(x, y)]$, 其中 $r_0(x, y)$ 的取值是 0 或 1.

$$o(x, y) = f(x, y)r(x, y) = \exp[i\pi f_0(x, y)] \cdot \exp[i\pi r_0(x, y)] \quad (1)$$

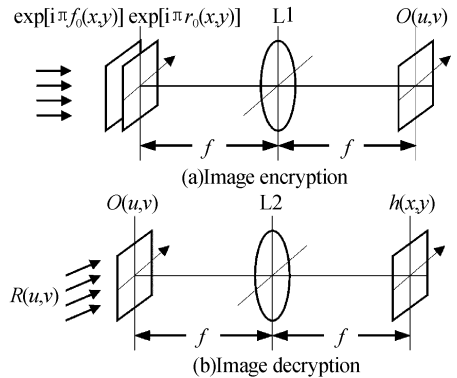


图1 随机相位编码的光实现

Fig. 1 Optical implementation of the random phase encryption
纯相位图像 $f(x, y)$ 与随机相位掩膜 $r(x, y)$ 在一束相干光的照射下, 经过透镜 L1 作傅里叶变换, 在 L1 的后焦面得到 $o(x, y)$ 的傅里叶变换 $O(u, v)$, 用全息图记录 $O(u, v)$.

$$O(u, v) = \text{FFT}[o(x, y)] = \text{FFT}[f(x, y)r(x, y)] \quad (2)$$

如果将式(2)的结果作为编码图像, 则解码的过程如图1(b)所示, 经过全息再现的编码图像 $O(u, v)$ 和一个平面参考光波 $R(u, v)$ 的干涉经过透镜 L2 作傅里叶反变换, $R(u, v) = \text{FFT}[r(x, y)]$, 设

$$H(u, v) = O(u, v) + R(u, v) \quad (3)$$

在 L2 的后焦面得到 $H(u, v)$ 的傅里叶反变换 $h(x, y) = o(x, y) + r(x, y)$, 记录其光强分布

$$|h(x, y)|^2 = |o(x, y) + r(x, y)|^2 = |o(x, y)|^2 + |r(x, y)|^2 + o^*(x, y)r(x, y) + o(x, y)r^*(x, y) \quad (4)$$

式中 * 号表示复数的共轭, 因为 $f(x, y)$ 和 $r(x, y)$ 都是纯相位图像, 式(4)可以简化为

$$|h(x, y)|^2 = 2 + 2\cos[\pi(f_0(x, y) + r_0(x, y))] \quad (5)$$

$$f_0(x, y) = \arccos[(|h(x, y)|^2 - 2)/2]/\pi \quad (6)$$

\arccos 表示反余弦函数, 经过式(6)的非线性变换, 可以完全重构原图像 $f_0(x, y)$.

在光学图像加密系统中, 一般解码及识别的过程要求快速而准确, 但是编码的速度不一定要很高, 为此可以先作非线性变换, 以加快解码速度. 设

*广东省自然科学基金(021089)、广东省教育厅自然科学基金项目(Z02020)资助

Tel: 020-85211361 Email: lirong1999@163.net

收稿日期: 2003-06-05

$f(x, y) = \exp [\text{i arccos} [(f_0(x, y) - 2)/2]]$, 则用式(4)可以直接解码得到原图像 $f_0(x, y)$.

1.2 实值编码方法

为了便于图像打印或者显示输出, 希望编码图像是一个实值的, 但是如果简单地将式(2)的实部作为编码图像, 用上述方法解码无法解出原图像. 设

$$H'(u, v) = \text{Re}[O(u, v)] + R(u, v) = O(u, v) + R(u, v) - \text{iIm}[O(u, v)] \quad (7)$$

根据二维离散傅里叶变换的对称性质^[6]

$$\begin{aligned} \text{FFT}[o(x, y) + o^*((N1 - x)_{N1}, \\ ((N2 - y)_{N2})]/2 &= \text{Re}[O(u, v)] \\ \text{FFT}[o(x, y) - o^*((N1 - x)_{N1}, \\ ((N2 - y)_{N2})]/2 &= \text{iIm}[O(u, v)] \end{aligned} \quad (8)$$

所以

$$h'(x, y) = o(x, y) + r(x, y) - \frac{1}{2}[o(x, y) - o^*((N1 - x)_{N1}, ((N2 - y)_{N2}))] \quad (9)$$

这里 $N1, N2$ 分别表示图像在 X, Y 轴方向的象素数, 即 x 的取值在 $[0, N1 - 1]$, y 的取值在 $[0, N2 - 1]$, $((n)_{N1})$ 表示整变量 n 对 N 取模运算. 为了书写方便, 用 $o'(x, y)$ 表示 $o((N1 - x)_{N1}, ((N2 - y)_{N2}))$, 并化简得

$$\begin{aligned} |h'(x, y)|^2 &= \frac{1}{4}|o(x, y)|^2 + |r(x, y)|^2 + \\ \frac{1}{4}|o'(x, y)|^2 &+ \frac{1}{2}[o(x, y)r^*(x, y) + o^*(x, y)r(x, y)] + \\ \frac{1}{4}[(o(x, y)o'(x, y) + o^*(x, y)o'^*(x, y))] &+ \\ \frac{1}{2}[o'(x, y)r(x, y) + o'^*(x, y)r^*(x, y)] &= \frac{1}{4}|o(x, \end{aligned}$$

$$\begin{aligned} y)|^2 + |r(x, y)|^2 + \frac{1}{4}|o'(x, y)|^2 + \text{Re}[o(x, y) \cdot \\ r^*(x, y)] + \frac{1}{2}\text{Re}[o(x, y)o'(x, y)] + \text{Re}[o'(x, y) \cdot \\ r(x, y)] \end{aligned} \quad (10)$$

将式(1)、(4)代入式(10)

$$\begin{aligned} |h'(x, y)|^2 &= \frac{1}{4} + 1 + \frac{1}{4} + \cos[\text{i}\pi f_0(x, y)] + \\ \frac{1}{2}\text{Re}[o(x, y)o'(x, y)] + \text{Re}[o'(x, y)r(x, y)] &= \\ \frac{3}{2} + \cos[\text{i}\pi f_0(x, y)] + \text{Re}[o'(x, y)r(x, y)] + \\ \frac{1}{2}\text{Re}[o(x, y)o'(x, y)] \end{aligned} \quad (11)$$

因为 $o'(x, y)$, 即 $o((N1 - x)_{N1}, ((N2 - y)_{N2}))$, 若忽略第一行和第一列, 则是 $o(x, y)$ 的反向图像, 式(11)中的第三、第四项与原图像没有函数关系, 所以按上述方法无法恢复原图像.

1.3 改进的解码方法

扩大编码范围, 原图像 $f_0(x, y)$ 只占待编码图像 $f(x, y)$ 的四分之一, $f(x, y)$ 用矩阵表示为

$$f(x, y) = \begin{bmatrix} \exp[\text{i}\pi f_0(x, y)] & \text{zero} \\ \text{zero} & \text{zero} \end{bmatrix} \quad (12)$$

$$o(x, y) = \begin{bmatrix} \exp[\text{i}\pi f_0(x, y)] \exp[\text{i}\pi r_0(x, y)] & \text{zero} \\ \text{zero} & \text{zero} \end{bmatrix} \quad (13)$$

$\text{zero}(x, y)$ 表示与原图像大小相同的全 0 矩阵, $\text{one}(x, y)$ 表示与原图像大小相同的全 1 矩阵, 若忽略第一行第一列, 则

$$o((N1 - x)_{N1}, ((N2 - y)_{N2})) = \begin{bmatrix} \text{zero} & \text{zero} \\ \text{zero} \exp[\text{i}\pi f_0((N1 - x)_{N1}, ((N2 - y)_{N2}))] \exp[\text{i}\pi r_0((N1 - x)_{N1}, ((N2 - y)_{N2}))] \end{bmatrix} \quad (14)$$

将式(12)、(13)、(14)代入式(10)

$$|h'(x, y)|^2 = \begin{bmatrix} \frac{5}{4} + \cos[\text{i}\pi f_0(x, y)] & \text{one} \\ \text{one} & \frac{5}{4} + \text{Re}[o((N1 - x)_{N1}, ((N2 - y)_{N2}))r(x, y)] \end{bmatrix} \quad (15)$$

由于式(12)左上角四分之一的矩阵是原图像的非线性函数, 经过变换可以解出原图像. 为了加快解码速度, 也可以先作非线性变换, 对式(16)的图像编码, 则可以直接译码得到原图像.

$$f(x, y) = \begin{bmatrix} \exp[\text{i arccos}[f_0(x, y) - \frac{5}{4}]] & \text{zero} \\ \text{zero} & \text{zero} \end{bmatrix} \quad (16)$$

2 计算机仿真

用 MATLAB 仿真软件进行计算机仿真,原图像是 64×64 像素的 lena 图像,图 2 所示是 1.1 节的基本算法仿真结果. 图 2(a)原图 $f_0(x, y)$, 图 2(b) 编码键 $r_0(x, y)$, 图 2(c)、(d) 分别是编码图像 $o(x, y)$ 实部和虚部, 图 2(e)、(f) 分别是解码键 $R(u, v)$ 的实部和虚部, 图 2(g)、(h) 分别是非线性变换前、后的解码图像. 为了加快解码速度, 先做非线性变换, 对图 2(i) 所示图像进行编码, 可以直接解码出图 2(h) 的图像. 图 2(j) 是错误的解码键解出的图像.

图 3 是 1.2 节的实值编码及解码算法仿真结果. 只取图 2(c) 所示 $o(x, y)$ 实部作为编码图像进行解码, 解出的图像如图 3, 可以看出不能解出原图像.

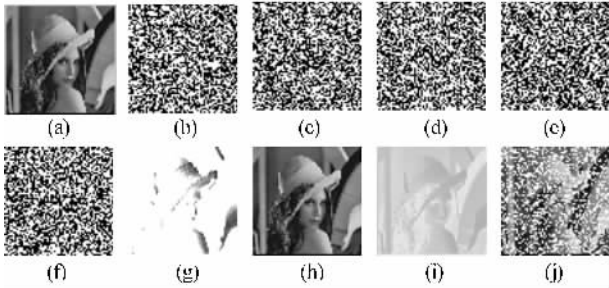


图 2 图像的复数编码译码方法

Fig. 2 Decryption with complex-pattern

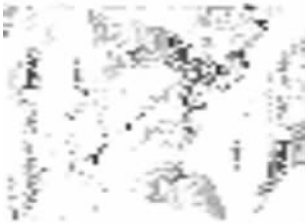


图 3 图像只取实部的解码图像

Fig. 3 Decryption with real part pattern

图 4 所示是 1.3 节的改进的实值编码及解码算法先作非线性变换仿真结果. 图 4(a)、(b) 分别是扩大图像 $f(x, y)$ 的实部和虚部, 图 4(c) 是编码键 $r_0(x, y)$, 图 4(d)、(e) 分别是编码图像实部和虚部, 图 4(f)、(g) 分别是解码键 $R(u, v)$ 的实部和虚部, 图 4(h) 是解码图像.

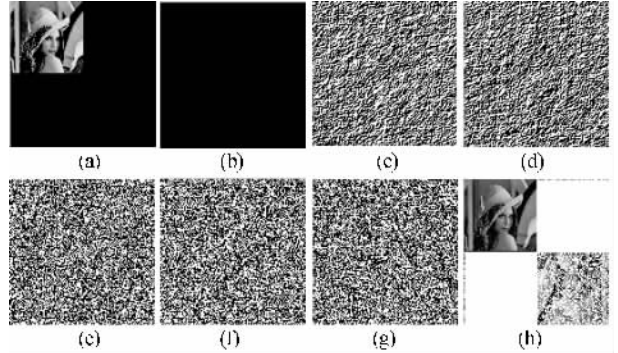


图 4 图像实值编码方法(先作非线性变换)

Fig. 4 The random phase real-value encryption and decryption method (Original image $f_0(x, y)$ is nonlinearly transformed by an arccosine function before encryption)

3 结论

本文分析了纯相位图像的实值编码, 提出了一种新的编码解码方法, 并进行了计算机仿真, 仿真结果表明, 该方法不仅可以得到实值的编码图像, 而且解码键与编码键相同, 编码和解码过程中只需要一个透镜作变换, 不需要频域滤波器, 光学系统简单.

参考文献

- 1 Javidi B, Ahouzi E. Optical security system with Fourier plane encoding. *Appl Opt*, 1998, **37**(26):6247 ~ 6255
- 2 Tan X, Matoba O, Shimura T, et al. Secure optical storage that uses fully phase encryption. *Appl Opt*, 2000, **39**(35):6689 ~ 6694
- 3 Mogensen P C, Glückstad J. Phase-only optical encryption. *Opt Lett*, 2000, **25**(8):566 ~ 568
- 4 Mogensen P C, Glückstad J. Phase-only optical encryption of a fixed mask. *Appl Opt*, 2001, **40**(8):1226 ~ 1235
- 5 Ohtsubo J, Fujimoto A. Practical image encryption and decryption by phase-coding technique for optical security systems. *Appl Opt*, 2002, **41**(23):4848 ~ 4855
- 6 [美] Dudgeon D E, Mersereau M 著. 多维数字信号处理. 北京: 科学出版社, 1991. 52 ~ 53
Dudgeon D E, Mersereau R M. *Multidimensional Digital Signal Processing*. Beijing: Science Press, 1991. 52 ~ 53

Optical Image Security Based on Random Phase Real-value Encryption

Li Rong, Li Ping

School of Physics and Telecommunications Engineering, South China Normal University, Guangzhou 510631

Received date: 2003-06-05

Abstract A random phase real-value encryption and decryption method is proposed for the optical image security system. A phase-only image to be encrypted together with a random phase mask is Fourier transformed and real part of the result is used as an encrypted image. The addition of encrypted image and the Fourier transformed of the random phase is inverse-Fourier transformed. The intensity of inverse-Fourier transformed image gives the exact original image. The method of encryption and decryption is simply performed and encrypted image is real-valued, so it is convenient for print or display on computer.

Keywords Optical image security; Random phase encryption; Real-value encryption



Li Rong received the M. S. degree from Northwestern Polytechnical University, Xi'an, China in 1989. He is now an associate professor in the School of Physics and Telecommunications Engineering, South China Normal University, China. His research interests include optical information processing, signal and image processing, communication systems.