第 54 卷 第 4 期 2005 年 4 月
1000-3290/2005/54(04)/1578-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.4,April,2005

双随机相位加密中相息图的优化设计*

杨晓苹[1)2)†] 翟宏琛[1)]

[1)](南开大学现代光学研究所,天津 300071)

[2)](天津理工大学光电信息与电子工程系,天津 300191)

(2003 年 12 月 19 日收到;2004 年 9 月 6 日收到修改稿)

采用基于记忆的模拟退火法对双随机相位加密中的相息图进行优化设计,并用该法分别对一个二元图像和一个灰度图像进行了模拟实验.实验结果表明,在不增大设计冗余度的情况下,运用该方法可降低相息图和密钥的相位量化带来的误差,得到与原加密图像质量几乎相同的解密图像.

关键词:基于记忆的模拟退火法,双随机相位加密,优化设计

PACC:4225F,4230K

1. 引 言

双随机相位加密方法[1—4]是用两个分别置于系统的输入和输出平面的随机相位将图像加密为白噪声,排除了在不知密钥的情况下对图像进行解密的可能性,此方法保密性较高,因而已被广泛地应用于光学图像防伪中,但由于需要同时纪录加密图像的振幅和相位信息,故解密图像时效率不高.而相息图[5]作为一种衍射光学元件,既可以获得任何期望的光强分布,又具有很高的衍射效率,将它应用于双随机相位加密系统中,可大大提高解密图像时的光学效率.

在相息图的设计中,迭代傅里叶算法(IFTA)[6]以其收敛速度快、寻优精度高等特点,得到了较为广泛的应用.但由于这种相位恢复问题的解析解在理论上是不存在的,因此在用 IFTA 设计相息图的过程中会发生迭代的停滞现象,使解密图像残留较大的散斑噪声,从而影响了解密图像的质量.可通过增加设计冗余度[7,8],即给图像周围增加一个无信号区的方法来解决迭代的停滞问题,但这会使相息图的光学效率下降.我们采用一种基于记忆的模拟退火法[9—12]对相息图进行设计,可在不增加设计冗余度情况下,降低由相息图和密钥的相位量化带来的解密图像和原始待加密图像之间的误差,提高了解密图像的质量,从而保证了相息图所具有的较高衍射效率的实现.

2. 加密和解密系统

本文采用文献[8]中的双随机相位加密系统,如图 1 所示.图 1 中的 $f(x)$ 表示待加密图像的复振幅分布,x 表示二维的像空间坐标,$p(x)$ 和 $b(v)$ 分别代表两个在 $[0,1]$ 之间均匀分布的二维随机阵列,FL1 和 FL2 为傅里叶透镜,$g(x)$ 为加密后的白噪声图像的复振幅分布,它仅是一个相位分布,即 $|g(x)|=c$,c 为任意常数.

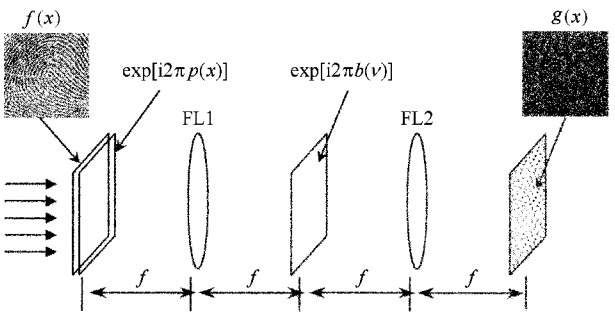

图 1 双随机相位加密系统

双随机相位加密系统的加密过程可表示为

$$g(x)=\mathrm{FT}^{-1}\{\mathrm{FT}[f(x)\exp[\mathrm{i}2\pi p(x)]]\times\exp[\mathrm{i}2\pi b(v)]\}=|g(x)|\exp[\mathrm{i}\psi(x)],\quad(1)$$

* 国家自然科学基金(批准号:60177004)资助的课题.

† E-mail:yangxiaoping@tsinghua.org.cn

式中，FT 为傅里叶变换，FT^{-1} 为傅里叶逆变换，$g(x)$的相位分布 $\psi(x)$及附加的相位分布 $b(v)$可以通过优化算法求出. $b(v)$一经确定，即可用 $H(u)=\exp[i2\pi b(v)]$作为从相息图 $g(x)$本身来恢复 $f(x)$的密钥. 由于 $p(x)$是随机噪声，因而 $b(v)$也是随机的，只不过这一随机相位的分布会与 $p(x)$和图像$f(x)$紧密相关. 所以，用 $H(u)$作为密钥有很高的安全性.

解密时仍可使用如图 1 所示的系统，只是此时输入平面是相息图 $g(x)$. 它经傅里叶变换后，在谱面上与密钥 $H(u)$的复共轭相乘，再经傅里叶逆变换就得到了被加密函数 $f(x)$与随机相位函数 $\exp[i2\pi p(x)]$的乘积. 由于通常情况下我们只关心解密图像的强度分布，取 $f(x)\exp[i2\pi p(x)]$的振幅，就可以得到被加密的图像 $f(x)$.

3. 用模拟退火法优化相息图

为制作出可实际应用的相息图和密钥，通常要求它们的相位取值是分等级量化的，亦即相息图和密钥的相位值只能取 $-\pi$ 和 $+\pi$ 之间的 Z 个等级 ($Z=2^n$, $n=1,2,3,\cdots$). 量化必然会使重建图像 $I(x,y)$和原始待加密图像 $f(x,y)$之间产生误差. 我们将这一误差用价值函数来表示，并将其定义为归一化的均方误差 E，

$$E=\frac{\iint ||f(x,y)|^2-\alpha I(x,y)|^2 \mathrm{d}x\mathrm{d}y}{\iint I(x,y)^2 \mathrm{d}x\mathrm{d}y}, \quad (2)$$

式中 α 为尺度因子，定义为

$$\alpha=\frac{\iint |f(x,y)|^2 \mathrm{d}x\mathrm{d}y}{\iint I(x,y)\mathrm{d}x\mathrm{d}y}. \quad (3)$$

显然，当重建图像趋于原始待加密图像时，E 趋于零.

一般而言，量化的阶数越高所带来的量化误差也就越小. 但我们并不能任意地选取量化阶数，而应在技术允许的范围内选取. 故将相息图的量化阶数取为 16 阶[13]，密钥的量化阶数取为 64 阶.

为降低由相位的量化带来的误差，我们提出用改进的模拟退火法即基于记忆的模拟退火法对相息图的相位值进行优化设计. 为此，我们给相息图的每一个像素逐一地引进一个微扰作为新解，即使该像素的相位值取 16 个量化阶中的任何一个，然后根据由冷却进度表确定的退火温度来计算价值函数，再根据接收准则来确定此微扰是否能够被接受. 所谓基于记忆的模拟退火法，即记住退火过程中最小的价值函数的值，并以此时的相息图和密钥作为最后的解. 这种方法可在有限的时间内得到较小的价值函数值，以使重建图像更趋于待加密图像. 图 2 为该算法的方框图，其迭代过程可描述如下：

(1) 将被加密函数 $f(x)$与一个随机相位函数 $\exp[i2\pi p(x)]$相乘，并将乘积作傅里叶变换，得到随机谱函数 $F(u)$.

(2) 作为迭代的原始输入，我们首先给 $b(v)$赋予一个随机的序列，将 $F(u)$与随机相位函数 $H(u)=\exp[i2\pi b(v)]$相乘，以使 $F(u)H(u)$经傅里叶逆变换后得到一个加密图像. 令此加密图像的振幅为常数，得到一个只有相位分布的加密相息图 $g(x)$，并以 $g(x)$作为迭代的原始相息图.

(3) 用 $H(u)$的复共轭作为密钥，对加密相息图 $g(x)$解密. 计算此解密图像与原始待加密图像的价值函数 E_{old}. 此时退火温度设置较高.

(4) 对相息图 $g(x)$的一个像素施加微扰，即将它的相位值用 16 阶相位值中的任一个来代替，得到新的加密相息图. 然后，以新的加密相息图作为输入重建图像，求出此时的价值函数 E_{new}.

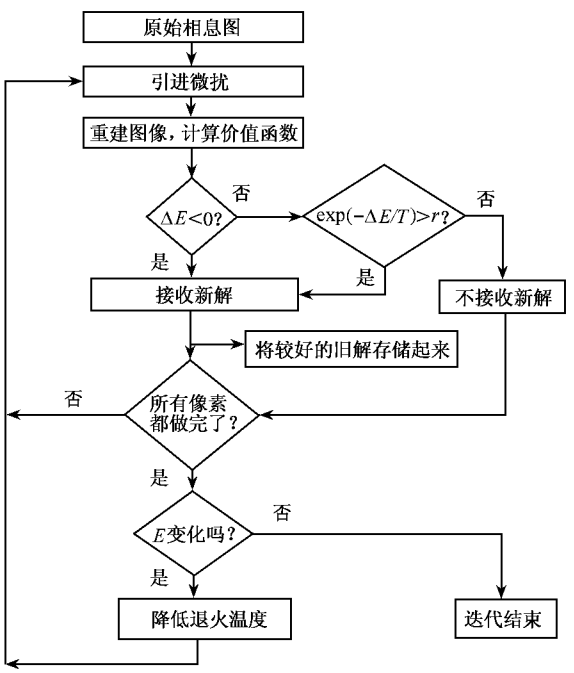

图 2　优化算法框图

(5) 计算引进微扰前后得到的两价值函数的差

$\Delta E = E_{new} - E_{old}$. 如果 $\Delta E < 0$, 接收此微扰 如果 $\Delta E > 0$, 则根据此时的退火温度计算接收概率 P,

$$P = \exp[-\Delta E/T], \quad (4)$$

式中 T 为退火温度. 如果 $P < r$ (r 为 0—1 之间的一个任意的随机数), 则不接收此微扰 ;而当 $P > r$ 时, 接收此微扰, 并同时将性能较好的旧解(即引进微扰前的相息图的相位分布及价值函数值)保留下来.

(6) 对相息图的每一个像素重复进行第(4)和第(5)步操作.

(7) 所有像素都做完后, 若 E 与上次迭代的 E 值不同, 则降低退火温度, 进行下一个周期的迭代. 如果 E 与上次迭代的 E 值相同, 则停止迭代.

(8) 取出记忆中最好的 E 值, 并用与之对应的相息图和以此相息图为基础求出的密钥的复共轭来重建图像.

4. 模拟实验及结果

我们在计算机上对上述优化算法进行了模拟实验. 实验所用的被加密图像为 64×64 像素的灰度指纹图像和一个二元图像, 相息图和密钥的大小亦为 64×64 像素, 相息图取 16 阶量化, 密钥取 64 阶量化, 实验结果如图 3 所示. 图 3(a),(b)为待加密图像, 图 3(c),(d)即为采用基于记忆的模拟退火法对相息图优化设计后所得到的重建图像, 由此可见, 此时解密图像的质量几乎与原图相同. 为便于比较, 我们应用文献[8]中的方法对同样的图像进行了加密, 由于迭代过程很快就趋于停滞, 从而使解密图像(如图 3(e),(f)所示)的质量较差.

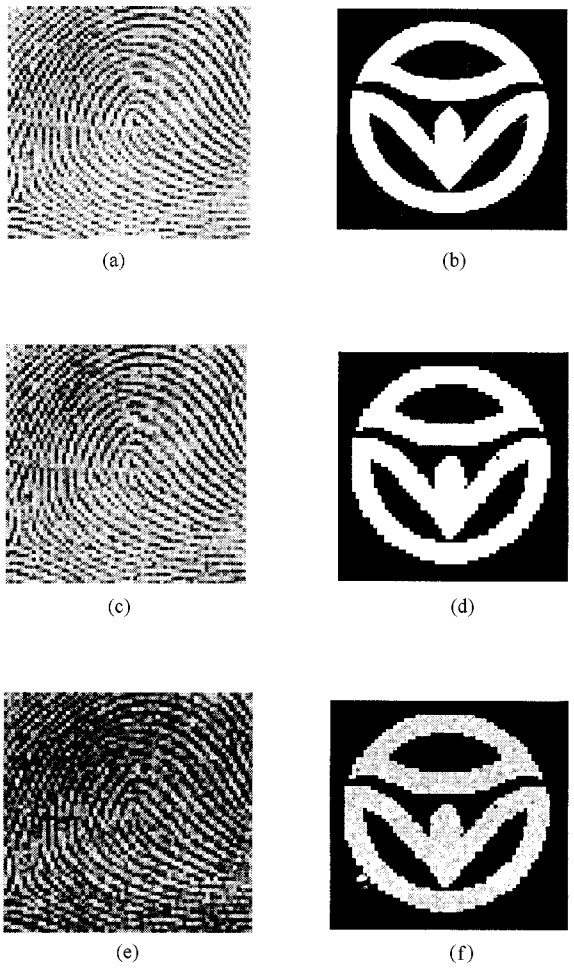

图 3 应用两种方法加密图像的结果比较 (a),(b)待加密图像 ;(c),(d)相息图优化后得到的重建图像 ;(e),(f)相息图没有优化时得到的重建图像

5. 冷却进度表的选取

由于冷却进度表的合理与否对模拟退火算法的算法进程以及算法是否收敛至关重要, 因此冷却进度表的选择是实验能否成功的关键所在. 实验时, 为找到合适的冷却进度, 我们根据冷却进度表的选取原则, 分别对两个加密图像采用了各不相同的三个冷却进度表进行了实验. 对于灰度的指纹图像, 温度 T 与迭代次数 N 的关系分别为

$$T = 1/(1 + N),$$
$$T = 1/(1 + N^{1.5}),$$
$$T = 1/\exp(N).$$

对于二元图像, 温度 T 与迭代次数 N 的关系分别为

$$T = 1/(1 + N^{1.5}),$$
$$T = 1/(1 + N^{3}),$$
$$T = 1/\exp(N).$$

图 4 为不同冷却进度表的价值函数 E 与迭代次数 N 的关系曲线. 由图 4 可见, 当迭代开始时各种降温方法的价值函数都随迭代次数的增加下降很快, 但随着迭代次数的增加它们的收敛情况各不相同.

对于二元图像, 当 $T = 1/\exp(N)$ 时, 迭代数次后价值函数就几乎不再变化, 说明此种冷却进度的降温速度太快, 因而难以达到全局最小 ;当 $T = 1/(1 + N^{1.5})$ 时, 迭代收敛很慢, 事实上, 在较多次(1000 次)的迭代后迭代仍不能收敛, 说明此时降温速度太慢, 也难以在有限的时间内达到全局最小 ;而当 $T = 1/(1 + N^{3})$ 时, 随着迭代次数的增加价值函数的值逐步减小, 直至在迭代数十次以后达到收敛, 说明此种降温速度比较合适. 将三种冷却进度下得到的记忆

中最优的解相比较，$T = 1/(1 + N^3)$时所得到的最优的价值函数值最小，此时得到的相息图即可作为系统的最优解.

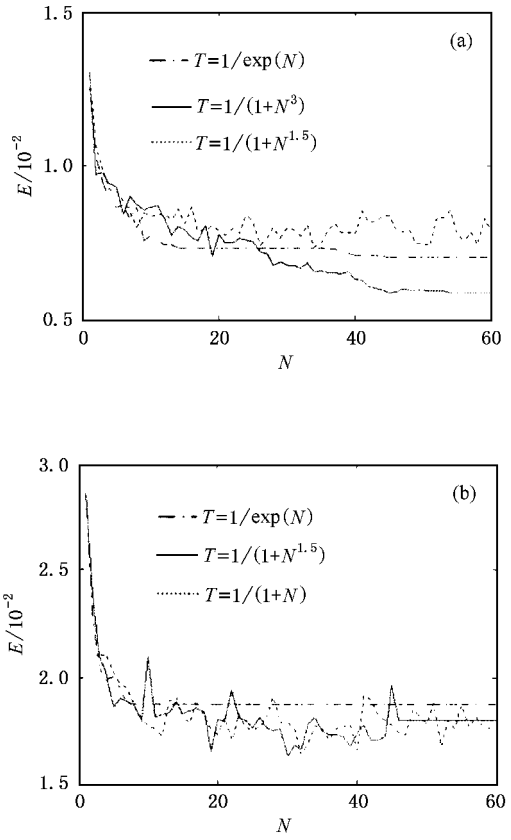

图 4　各种冷却进度时重建像的价值函数 E 与迭代次数 N 的关系　(a) 对二元图像加密时，(b) 对灰度图像加密时

对于灰度图像，当 $T = 1/\exp(N)$时，同样在迭代数次后其价值函数就达到了停滞状态；当 $T = 1/(1 + N)$时，迭代收敛很慢，在较多次(1000 次)的迭代后也是不能收敛，说明此时降温速度太慢；对于 $T = 1/(1 + N^{1.5})$，与二元图像加密时的情形完全不同，此时价值函数在经过数十次的迭代后就可以收敛，同时其记忆中的最小价值函数值是这三种降温方法中最好的，此时得到的解就可以作为系统的最优解.

由上述实验和分析可见，在将模拟退火法应用于实际的随机相位加密问题时，冷却进度表将控制算法进程的收敛情况，尽管使用的是同样的加密和解密系统，但由于所加密的图像对象不同，我们所得到的结果与算法进程都是不同的.因此，对于每一个要应用的对象，在选取冷却进度表时都应该具体问题具体分析，进行多次实验后确定一个合适的函数形式，找到最合适的冷却进度，从而得到问题真正的最优解.

6. 结　论

本文将基于记忆的模拟退火法应用于双随机相位图像加密中相息图的优化设计，并运用该方法对一指纹图像和一个二元图像进行了模拟实验.实验结果表明，应用基于记忆的模拟退火优化方法，可在不增加图像周围无信号区即不增加设计自由度的情况下，得到与原加密图像质量几乎相同的解密图像.模拟退火法的缺点是需要较长的计算时间，但由于相息图的设计可以离线进行，因此并不影响该方法在光学信息加密中的使用.

[1] Javidi B, Sergent A, Zhang G *et al* 1997 *Opt. Eng.* **36** 992

[2] Zhai H C, Liu F M, Yang X P *et al* 2003 *Opt. Commun.* **219** 81

[3] Unnikrishnan G, Singh K 2001 *Opt. Commun.* **193** 51

[4] Liu S T, Yu L, Zhu B H 2001 *Opt. Commun.* **187** 57

[5] Jin G F, Yan Y B, Wu M X *et al* 1999 *Binary Optics* (Beijing: National Defence Indrstry Press) Chap. 1 (in Chinese) [金国藩、严瑛白、邬敏贤等 1999 二元光学(北京：国防工业出版社)第 1 章]

[6] Liu F M, Zhai H C, Yang X P *et al* 2003 *Acta Opt. Sin.* **23** 666 (in Chinese) [刘福民、翟宏琛、杨晓苹等 2003 光学学报 **23** 666]

[7] Wyrowski F 1990 *J. Opt. Soc. Am.* A **7** 961

[8] Liu F M, Zhai H C, Yang X P 2003 *Acta Phys. Sin.* **52** 2462 (in Chinese) [刘福民、翟宏琛、杨晓苹 2003 物理学报 **52** 2462]

[9] Arrizon V, Gonzalez L A 2000 *Opt. Commun.* **180** 247

[10] Roa-Sepulveda C A, Pavez-Lazo B J 2003 *Int. J. Electr. Power Energy Sys.* **25** 47

[11] Yu Z X, Mo D 2003 *Thin Solid Films* **425** 108

[12] Meister M, Winfield R J 2002 *Opt. Commun.* **203** 39

[13] Yan S H, Dai Y F, Lü H B *et al* 2002 *Semicon. Optoelectr.* **23** 159 [颜树华、戴一帆、吕海宝等 2002 半导体光电 **23** 159]

Optimization of kinoform in double-random-phase encryption*

Yang Xiao-Ping[1)2)] Zhai Hong-Chen[1)]

[1)] (*Institute of Modern Optics, Nankai University, Tianjin* 300071, *China*)

[2)] (*Department of Photoelectronics, Tianjin University of Technology, Tianjin* 300191, *China*)

(Received 19 December 2003; revised manuscript received 6 September 2004)

Abstract

In this paper, the design of kinoforms in double-random-phase encryption method is optimized by the memory-based simulated annealing technique, which is applied to the simulation experiment of a binary image and an image with gray levels. The results of the experiments show that, without increasing the abundance of design, the errors caused by the quantization of phases of kinoform and key is decreased, and almost the same image quality as the original one is obtained as a decoded image by the proposed method.

Keywords: memory-based simulated annealing technique, double random phase encryption, design optimization

PACC: 4225F, 4230K

* Project supported by the National Natural Science Foundation of China (Grant No. 60177004).