文章编号 1004-924X(2007)04-0577-05

基于 JTC 的光学加密系统密钥设计新方法

吴克难,胡家升,林 勇
(大连理工大学 电子与信息工程学院,辽宁 大连 116024)

摘要:分析总结了基于 JTC 的光学加密系统密钥设计问题,提出了采用模糊控制迭代算法来代替 G-S 算法生成密钥,并与利用 G-S 算法和平滑修正法所得密钥进行了对比。理论计算和计算机模拟实验结果显示,模糊控制迭代算法的迭代结果其振幅均方误差为 0.69%,振幅不均匀度为 1.01%。采用模糊控制迭代算法生成的密钥解密质量优于 G-S 算法和平滑修正法。

关 键 词:光学加密;JTC;模糊控制迭代算法
中图分类号:TP309.7 **文献标识码**:A

A novel method of key design in optical encryption system based on JTC architecture

WU Ke-nan, HU Jia-sheng, LIN Yong

(*School of Electronics and Information Engineering, Dalian University of Technology, Dalian* 116024, *China*)

Abstract: After analyzing and summarizing the problem of key design in JTC encryption system, an Iterative Algorithm based on Fuzzy Control Theory (IAFC) in place of G-S was proposed, and the comparison with G-S and Sleek Revise(SR) algorithms was given. Computer simulation experiment, as well as theoretical research show that the amplitude mean square error of the iterative output derived from IAFC is 0.69%, and the amplitude un-uniformity is 1.01%. Therefore the decryption quality of key design from IAFC is better than that of key designed from G-S and SR algorithms.

Key words: optical encryption; JTC; Iterative Algorithm based on Fuzzy Control Theory (IAFC)

1 引 言

1995 年,Refregier 和 Javidi 提出了双随机相位编码技术(double random phase encoding)[1]来加密图象信息,这种方法结构简单,同时具有较高的安全性,因此引起了广泛关注。然而,一些缺陷影响了它的广泛应用。比如,双随机相位加密系统在结构上基于 4f 图像处理系统,两个相位掩模必须在空间位置上精确对准;再者,双随机相位加密系统的加密结果为复分布,难以记录及传输。于是研究者分别提出了基于联合变换相关器[2](JTC)的光学加密系统[3-4]和利用数字全息[5-6]的加密方法[7-8]试图解决上述问题。

在基于 JTC 的光学加密系统中,密钥被放置在输入平面,为了使解密信息和原始图象信息一

收稿日期:2007-01-22;**修订日期**:2007-02-18.
基金项目:大连市政府资助项目(No. 2006A14GX044)

致，密钥频谱的振幅必须均匀。另外，密钥本身要求是纯相位掩模，并被限制在一个有限的区域内。为了得到满足这些要求的密钥，可以利用各种迭代算法，其中目前最常采用的迭代算法为 G-S 算法。采用 G-S 算法设计密钥，可以迅速降低迭代结果的振幅均方误差 MSE，但信号区振幅不均匀度较大。为此有人利用函数插值法为 G-S 算法选取迭代前的初始相位分布，以改善迭代结果[9,10]。

作者的目标是得到同时具有较小的振幅均方误差 MSE 和信号区振幅不均匀度 σ 的迭代结果，作为 JTC 加密系统的密钥。这是一个多目标优化问题，可以利用模糊控制迭代算法(IAFC)解决。模糊控制迭代算法根据模糊控制理论，智能地在每轮迭代中采用不同算法。本文将模糊控制迭代算法用于 JTC 加密系统的密钥设计。计算机模拟实验结果表明，模糊控制迭代算法的迭代结果同时具有较小的振幅均方误差和振幅不均匀度，这种方法设计的密钥解密质量较好。

2　基于 JTC 的加密系统的密钥设计

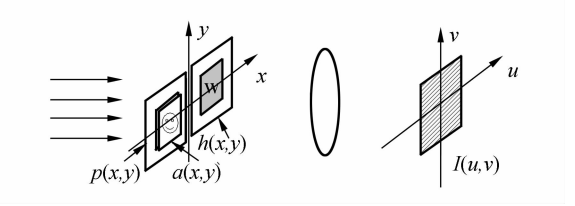
基于 JTC 的加密系统由 Nomura 和 Javidi 于 2000 年提出[3,4]，其原理如图 1 所示。在加密过程中，首先将要加密的原始图像 $a(x,y)$ 和一个随机相位散射体(random phase diffuser) $p(x,y)$ 叠放在一起，然后二者再与密钥掩模 $h(x,y)$ 分别放置在坐标 $(-x_0,0)$ 和 $(x_0,0)$ 处。利用 JTC 得到它们的联合变换功率谱 $I(u,v)$ 就是密文信息。

$$\begin{aligned}I(u,v)=&|\mathrm{FT}\{a(x+x_0,y)p(x+x_0,y)+h(x-x_0,y)\}|^2=\\&|A(u,v)*P(u,v)|^2+|H(u,v)|^2+\\&[A(u,v)*P(u,v)]H^*(u,v)e^{j4\pi x_0u}+\\&[A(u,v)*P(u,v)]^*H(u,v)e^{-j4\pi x_0u}\end{aligned},\quad(1)$$

其中 $\mathrm{FT}\{\cdot\}$，$\{\cdot\}^*$，$\{\cdot\}*\{\cdot\}$ 分别表示傅里叶变换运算，复共轭运算和卷积运算。$A(u,v)$，$P(u,v)$，$H(u,v)$ 分别表示 $a(x,y)$，$p(x,y)$，$h(x,y)$ 的傅里叶变换。在解密过程中，$h(x,y)$ 被放置在输入平面坐标 $(x_0,0)$ 处，用来解密位于频谱面的密文信息 $I(u,v)$。解密信息由公式(1)中第 3 项得到。

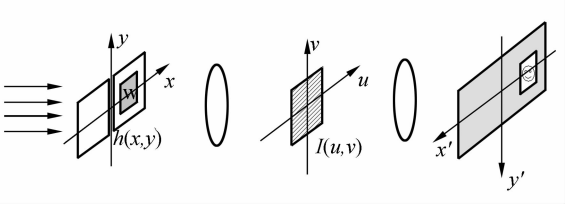
$$\begin{aligned}a_{r3}(x',y')=&\mathrm{IFT}\{H(u,v)e^{-j2\pi x_0u}\cdot\\&[A(u,v)*P(u,v)]H^*(u,v)e^{j4\pi x_0u}=\\&[a(x',y')p(x',y')]*\\&\mathrm{IFT}\{|H(u,v)|^2\}*\delta(x'+x_0,y')\end{aligned},\quad(2)$$

其中 $\mathrm{IFT}\{\cdot\}$ 代表逆傅里叶变换，$\delta(\cdot)$ 代表 Dirac 函数。



(a)加密过程

(a) Encryption process



(b) 解密过程

(b) Decryption process

图 1　基于 JTC 结构的加密系统

Fig. 1　Optical encryption system based on JTC architecture

从公式(2)可以看出，为了使解密信息和原始图像信息一致，要求在 JTC 结构的频谱面上的 $|H(u,v)|=c$，c 为常数，即 $H(u,v)$ 的振幅为均匀分布。从图 1(a)又可以看出，密钥掩模 $h(x,y)$ 被限制在一个有限区域 W 内，是空间受限的。因此，基于 JTC 结构加密系统的密钥设计问题就转化为寻找纯相位函数 $H(u,v)=c\mathrm{e}^{i2\pi\Phi(u,v)}$ 及它的逆傅里叶变换 $h(x,y)=|h(x,y)|\,\mathrm{e}^{i2\pi\phi(x,y)}$，使其满足：

$$|\mathrm{IFT}[H(u,v)]|=|h(x,y)|\approx A(x,y)=\begin{cases}1 & |x|\leqslant\Delta X,|y|\leqslant\Delta Y\\0 & \text{otherwise}\end{cases},\quad(3)$$

其中 c 根据能量守恒原则确定，ΔX，ΔY 为限制区域 W 的大小。均方误差 MSE 和顶部振幅不均匀度 σ 经常用来评价 $h(x,y)$ 满足方程(1)的程度。

$$\mathrm{MSE}=\frac{\sum\limits_{x,y}\|\,h(x,y)\,|-A(x,y)\,|^2}{\sum\limits_{x,y}|\,A(x,y)\,|^2},\quad(4)$$

$$\sigma=\sqrt{\sum_{(x,y)\in W}\left[\frac{|h(x,y)|-\bar{h}}{\bar{h}}\right]^2/(n-1)}\ ,\quad(5)$$

$$\bar{h}=\sum_{(x,y)\in W}|h(x,y)|/n$$

其中 n 表示区域 W 中采样点数量。从上两式可以看出，MSE 值主要反映 $|h(x,y)|$ 和 $A(x,y)$ 的接近程度，而 σ 值主要反映位于限制区域 W 内的 $|h(x,y)|$ 的平滑程度。

3　算法描述

如前所述，JTC 加密系统的密钥设计问题是一个多目标优化问题，可以利用模糊控制迭代算法解决。本文将利用这种方法进行 JTC 加密系统的密钥设计。

模糊控制迭代算法以 G-S 算法[11]和平滑修正法为基础。平滑修正法和 G-S 算法流程相似，它与 G-S 算法的区别在于，每次迭代只将限制窗 W 中 $|h(x,y)|$ 均匀性相对较差的 $h(x,y)$ 修正为 $A(x,y)$。具体修正方式如公式(8)(9)所示。

G-S 算法的迭代结果往往收敛于某一局部最小值，此时 $|h(x,y)|$ 在限制窗 W 中的均匀性较差，σ 值比较大。平滑修正法可以迅速降低 σ 值，但得到的 MSE 值较大。

模糊控制迭代算法根据 MSE 值和 σ 值智能地控制整个迭代过程。首先随机选定一个初始分布 $H_0(u,v)=\exp[i2\pi\Phi_0(u,v)]$，然后对 $H_0(u,v)$ 进行傅里叶变换得到 $h_0(u,v)$，并计算 $h_0(u,v)$ 的 MSE 值和 σ 值，依据模糊控制理论，如果 MSE 值相对 σ 值大，则本次迭代采用 G-S 算法；如果 MSE 值相对 σ 值小，则本次迭代采用平滑修正法，然后进行下一轮迭代。一般地，第 k 轮迭代过程可以表示为：

$$h_k=|h_k|\exp(i\phi_k)=\mathrm{FT}\{H_k\}\ ,\quad(6)$$

如果 MSE 值相对 σ 值大

$$\tilde{h}_k=|\tilde{h}_k|\exp(i\phi_k)=A(x,y)\exp(i\phi_k)\ ,\quad(7)$$

如果 MSE 值相对 σ 值小

$$\tilde{h}_k=|\tilde{h}_k|\exp(i\phi_k)=D(x,y)\exp(i\phi_k)\ ,\quad(8)$$

$$D(x,y)=\begin{cases}A(x,y) & (x,y)\in W\ ,\\ & ||h_t(x,y)|-\overline{|h_t(x,y)|}|>\text{threshold}\\ |h_t(x,y)| & \text{otherwise}\ ,\end{cases}\quad(9)$$

$$\widetilde{H}_k=|\widetilde{H}_k|\exp(i\Phi_k)=\mathrm{IFT}\{\tilde{h}_k\}\ ,\quad(10)$$

$$H_k=|H_k|\exp(i\Phi_k)=\exp\{i\Phi_k\}\ ,\quad(11)$$

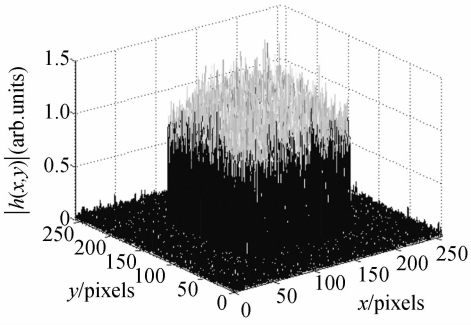
迭代收敛时的 h_k 就是所期望的密钥。

4　计算机模拟实验

在基于 JTC 的加密系统中，设原始图像 $a(x,y)$ 的分辨率为 256×256，如图 2 所示，限制在区域 W 内的密钥采样点数为 128×128。为了进行对比，分别利用 G-S 算法、平滑修正法、模糊

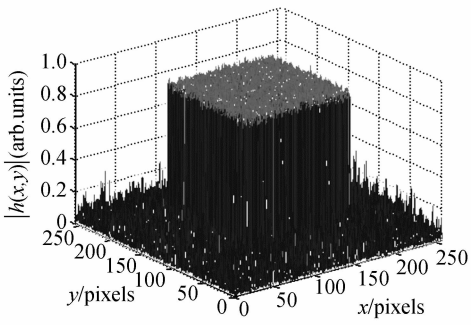
图 2　原始图象 $a(x,y)$

Fig. 2　Original image $a(x,y)$



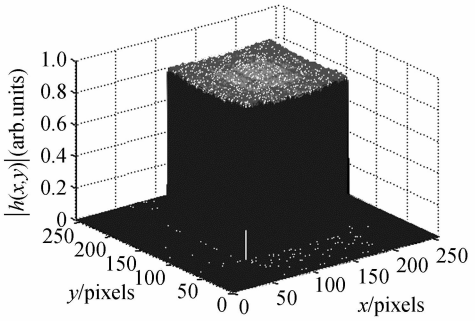
(a) G-S 算法

(a) G-S algorithm



(b) 平滑修正法

(b) SR algorithm



(c) 模糊控制迭代算法

(c) IAFC

图 3　三种算法得到的$|h(x,y)|$分布

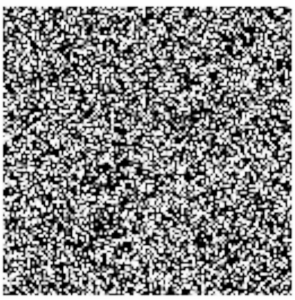
Fig. 3　Distribution of $|h(x,y)|$ obtained by three algorithms

控制迭代算法设计密钥。三种算法得到的$|h(x,y)|$分别如图 3(a),(b),(c)所示,对应的 MSE 值和σ值如表 1 所示。三种方法设计的密钥及解密结果则展示在图 4 和图 5 中。

表 1　三种算法迭代结果比较

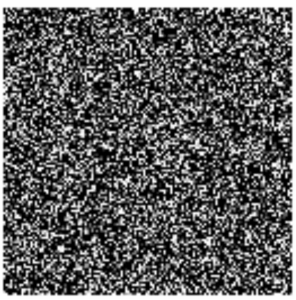
Tab. 1　Results comparison of three algorithms

	MSE(%)	σ(%)
G-S	2.77	16.20
Sleek Revise algorithm	2.32	2.22
IAFC	0.69	1.01



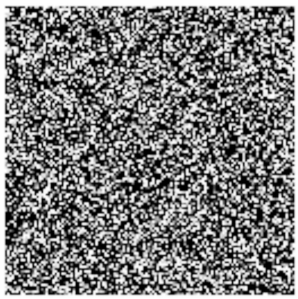
(a) G-S 算法

(a) G-S algorithm



(b) 平滑修正法

(b) SR algorithm



(c) 模糊控制迭代算法

(c) IAFC

图 4　三种方法设计的密钥

Fig. 4　Keys designed by three algorithms

(a) G-S 算法

(a) G-S algorithm

(b) 平滑修正法

(b) SR algorithm

(c) 模糊控制迭代算法

(c) IAFC

图 5　三种方法设计密钥的解密图象

Fig. 5　Decrypted images using keys designed by three algorithms respectively

5　结　论

在基于 JTC 的光学加密系统中，要求密钥频谱的振幅必须均匀，同时密钥掩模被限制在一个有限的空间区域内。本文针对上述要求，利用模糊控制迭代算法生成密钥，得到了较为理想的结果。

本文对 G-S 算法，平滑修正法，模糊控制迭代算法进行了对比。计算机模拟实验结果表明，G-S 算法可以迅速降低 MSE 值，但得到的 σ 值相对较大；而利用平滑修正法可以迅速降低 σ 值，但得到的 MSE 值较大；模糊控制迭代算法较为智能地结合了二者的长处，迭代结果振幅均方误差为 0.69%，振幅不均匀度为 1.01%，二者均较小。采用模糊控制迭代算法生成密钥，所得解密图象质量优于 G-S 算法和平滑修正法。

参考文献：

[1] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Opt. Lett.*, 1995, 20(7): 767-769.

[2] 王玉荣，徐鹏，王青圃，等. 光电混合联合变换相关器中各元器件结构参数之间的关系[J]. 光学 精密工程，2005，13(3)：376-384.
WANG Y R, XU P, WANG Q P, *et al*.. Relationship between parameters in hybrid optical/electronic joint transform correlator[J]. *Opt. Precision Eng.*, 2005, 13(3): 376-384. (in Chinese)

[3] NOMURA T, JAVIDI B. Optical encryption using a joint transform correlator architecture[J]. *Opt. Eng.*, 2000, 39(8): 2031-2035.

[4] NOMURA T, JAVIDI B. Optical encryption system with a binary key code[J]. *Appl. Opt.*, 2000, 39(26): 4783-4787.

[5] 潘武，田贻丽. 光学全息的数字实现[J]. 光学 精密工程，2005，13(增)：15-20.
PAN W, TIAN Y L. Digital implementation scheme of optical holograms[J]. *Opt. Precision Eng.*, 2005, 13(Supp.): 15-20. (in Chinese)

[6] 周文静，彭娇，于瀛洁. 基于数字全息技术的变形测量[J]. 光学 精密工程，2005，13(增)：46-51.
ZHOU W J, PENG J, YU Y J. Deformation measurement via digital holography[J]. *Opt. Precision Eng.*, 2005, 13(Supp.): 46-51. (in Chinese)

[7] JAVIDI B, NOMURA T. Securing information by use of digital holography[J]. *Opt. Lett.*, 2000, 25(1): 28-30.

[8] NISHCHAL N, JOSEPH J, SINGH K. Securing information using fractional Fourier transform in digital holography[J]. *Opt. Commun.*, 2004, 235(4-6): 253-259.

[9] CHENG CH J, LIN L CH, WANG CH M, *et al*.. Optical joint transform encryption using binary phase difference key mask[J]. *Opt. Rev.*, 2005, 12(5): 367-371.

[10] LIN L CH, CHENG CH J. Optimal key mask design for optical encryption based on joint transform correlator architecture[J]. *Opt. Commun.*, 2006, 258(2): 144-154.

[11] THOMSON M J, LIU J S, TAGHIZADEH M R. Iterative algorithm for the design of free-space diffractive optical elements for fiber coupling[J]. *Appl. Opt.*, 2004, 43(10): 1996-1999.

作者简介：吴克难(1984－)，男，辽宁抚顺人，博士研究生，主要研究方向为成像科学与图象处理，信息安全与防伪技术。E-mail: zhang_liu73@163.com;

胡家升(1941－)，男，辽宁昌图人，大连理工大学教授，博士生导师，研究方向为工程光学，成像科学与图象处理，光学系统设计，信息安全与防伪技术，X 射线成像技术等，在上述领域发表论文逾百篇。E-mail: jshu@dlut.edu.cn