

基于级联迭代傅里叶变换算法的光学安全技术

容 强

(郑州轻工业学院 易斯顿美院,河南 郑州 451450)

摘 要:基于级联迭代傅里叶(CIFT)变换算法提出了一种新的光学图像的加密方法,该方法通过输入和4-F相关的傅里叶域的模糊设计和定位,从而实现光学加密以及真实性验证。与以往的方法有所不同,新算法采用改进的搜索策略:修改两个阶段的同步分布,同时扩大搜索空间。计算机模拟实验表明其快速的收敛算法能够更好地恢复图像的质量,密钥会被分配到不同的方面,用户只有在得到这些密钥的授权之后才能得到解密后的图像,这种密钥分配策略可以极大减少被入侵的风险。

关键词:光学安全;光学加密;级联迭代傅里叶变换算法

中图分类号:TP301.6

文献标识码:A

文章编号:1673-629X(2014)02-0168-04

doi:10.3969/j.issn.1673-629X.2014.02.041

Optical Security Technology Based on Cascaded Iterative Fourier Transform Algorithm

RONG Qiang

(Eastern Art College, Zhengzhou College of Light Industry, Zhengzhou 451450, China)

Abstract: A Cascaded Iterative Fourier Transform (CIFT) algorithm is presented for optical security applications. Two phase-masks are designed and located in the input and the Fourier domains of a 4-F correlator respectively, implementing the optical encryption or authenticity verification. Compared with previous methods, the proposed algorithm employs an improved searching strategy: modifying the phase-distributions of both masks synchronously as well as enlarging the searching space. Computer simulations show that the algorithm results in much faster convergence and better image quality for the recovered image. Each of these masks is assigned to different person. Therefore, the decrypted image can be obtained only when all these masks are under authorization. This key-assignment strategy may reduce the risk of being intruded.

Key words: optical security; optical encryption; cascaded iterative Fourier transform algorithm

0 引言

光学技术在信息安全领域的应用潜力巨大,目前常用的是一种双随机相位编码技术,它将主图像编码成一个固定的白噪声。而文中提出的光学加密和真实性核查是另一种方法,用这种方法加密信息,位于输入或4-F相关器 Fourier 域时,完全变成了相位掩模。4-F光学系统是个十分典型的相干滤波系统(见图1),相当于进行了两次傅里叶变换,它通过不同的滤波器对频谱面上输入函数的频谱进行修改,过滤掉不需要的信息和噪声,而保留或增强有用的信息,并对第二个透镜做逆傅里叶变换,使得输出函数产生预期目的的变换^[1]。由于在频谱面的空间滤波器可以对输入函数

频谱的振幅和相位进行调节,因此,4-F系统可以用于图像的编码和识别,也可用于图像加密。例如,给定一个显著图像 $F(X,Y)$ 的预定义在傅里叶域所需的输出和相位分布 $\text{EXP}\{\text{IB}(U,V)\}$,可以很容易地用一个改进的约束集投影(POCS)算法优化其他相位函数 $\text{EXP}\{\text{IP}(X,Y)\}$ ^[2-3]。因此,图像 $F(X,Y)$ 被编码成 $\text{EXP}\{\text{IP}(X,Y)\}$ 与 $\text{EXP}\{\text{IB}(U,V)\}$ 。换言之,固定相 $\text{EXP}\{\text{IB}(U,V)\}$ 作为锁,而检索阶段 $\text{EXP}\{\text{IP}(X,Y)\}$ 作为安全系统的关键。重建的原始信息,相函数 $\text{EXP}\{\text{IP}(X,Y)\}$ 和 $\text{EXP}\{\text{IB}(U,V)\}$,必须在输入和傅里叶平面分别与之匹配。

然而,由于键 $\text{EXP}\{\text{IP}(X,Y)\}$ 中包含图像的 $F(X,Y)$ 的信息和锁定 $\text{EXP}\{\text{IB}(U,V)\}$,以及4-F相

收稿日期:2013-03-18

修回日期:2013-06-25

网络出版时间:2013-11-12

基金项目:河南省重点科技攻关项目基金(132102310003)

作者简介:容 强(1971-),男,讲师,硕士,研究方向为信息安全、嵌入式应用、多媒体技术等。

网络出版地址:<http://www.cnki.net/kcms/detail/61.1450.TP.20131112.1650.042.html>

关器具有线性的特性,如果该系统仅使用一个不同的图像锁定功能,它有可能成为入侵者通过统计分析的随机字符的按键找出锁的相分布^[4]。为了提高这类系统的安全级别,一种方法是为不同的图像使用不同的锁定功能;另一种方法是扩大主要空间以提高安全水平^[5-6]。它可以实现加密的分数傅里叶域图像,最终为规模因子和变换顺序提供额外的钥匙。另一方面,相位掩模作为该系统的关键,扩大密钥空间可以在目标图像编码成两个或多个相位掩模。一个多阶段的检索算法虽然在光学安全系统基础上解密图像具有较高的安全性和更高的质量水平,然而这种算法检索在每次迭代的阶段约束只有一个相分布,由于掩码不太一致,可能会影响恢复图像的质量^[7]。

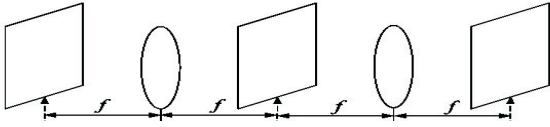


图1 4-F体系结构的光学安全系统

可以通过一种改进的POCS算法,在每一次迭代过程中同时调整相位掩模同步分布。迭代过程的收敛速度有望显著增加,在迭代过程中的两个掩码调整,更高质量的目标图像有望复苏。当迭代过程完成后,目标图像编码成相位掩码成功,这些掩码作为每个服务器安全系统的密钥和加密图像的本身以及一部分。此外,该算法可以扩展到多个相关器的任意阶段相位掩码,获得最大的安全性,每个键被分配不同的权限,未被授权的人无法进行解密。

1 级联迭代傅里叶变换算法(CIFT)

考虑加密系统的操作与4-F相关器,放置在输入和傅里叶平面相位掩码是FOPT(X, Y)和WOPT(U, V),其中(X, Y)和(U, V)分别代表空间和频率坐标。一旦系统照亮单色平面波,目标图像 $F(X, Y)$ 有望在输出平面获得,相位掩码FOPT(X, Y)和WOPT(U, V)包含了信息 $F(X, Y)$,是 $F(X, Y)$ 被编码到这些阶段的

$$R(k) = \frac{\sum_{m=1}^M \sum_{n=1}^N \{f(m, n) - E[f]\} \{f_k(m, n) - E[f_k]\}}{\left\{ \left\{ \sum_{m=1}^M \sum_{n=1}^N [f(m, n) - E[f]]^2 \right\} \left\{ \sum_{m=1}^M \sum_{n=1}^N [f_k(m, n) - E[f_k]]^2 \right\} \right\}^{1/2}} \quad (6)$$

其中, $M * N$ 表示图像的大小; $E[\cdot]$ 表示图像的平均值。该算法的收敛行为类似于常规的POCS。也就是说,在MSE中最重要的几个迭代骤减,然后慢慢减少,直到它达到最低。相应地,最初相关系数预计迅速增加,并保持缓慢增加,直到满足停止准则。

解码确定相位掩码FOPT(X, Y)和WOPT(U, V)分别被放置在输入和傅里叶平面,然后通过定义关联式转化成输出平面,输出模是解密图像。CIFT算法分阶段

掩码^[8-10]。编码过程是两阶段分布的优化,问题归结为在三维检索沿传播方向的平面,传统的POCS算法应该被修改。

级联迭代傅里叶变换算法(CIFT)开始初始化与相位掩码分布。假设迭代过程到达第 K 次迭代($K = 1, 2, \dots$),在输入和傅里叶平面分阶段分布分别代表 $F_k(X, Y)$ 和 $W_k(U, V)$ 。然后在定义的相关器下输出获得的目标图像。

$$f_k(x, y) \exp[i\varnothing_k(x, y)] = \text{IFT}\{\text{FT}\{\exp[i2\pi\varnothing_k(x, y)]\} * \exp[i2\pi\varphi_k(u, v)]\} \quad (1)$$

FT和IFT分别表示傅里叶变换和傅里叶逆变换。 $F_k\{X, Y\}$ 如果满足收敛准则,进程停止, QOPT(X, Y) = $Q_k(X, Y)$ 和WOPT(U, V) = $W_k(U, V)$ 是优化分布。否则, $F_k(X, Y)$ 修改,以满足目标图像约束如下

$$f'_k = \begin{cases} f(x, y), & \text{if } f(x, y) > 0 \\ f_k(x, y), & \text{if } f(x, y) = 0 \end{cases} \quad (2)$$

功能转化后产生的两个相位分布如下

$$\varphi_{k+1}(u, v) = \text{ang}\left\{\frac{\text{FT}\{f'_k(x, y) \exp[i\varnothing_k(x, y)]\}}{\text{FT}\{\exp[i2\pi\varnothing_k(x, y)]\}}\right\} \quad (3)$$

或

$$\varnothing_{k+1}(x, y) = \text{ang}\left\{\frac{\text{FT}\{f'_k(x, y) \exp[i\varnothing_k(x, y)]\}}{\exp[i2\pi\varphi_k(u, v)]}\right\} \quad (4)$$

$\text{ang}\{\cdot\}$ 表示相萃取功能。则 K 是由 $K+1$ 代替,为下一次迭代。据式(3)、(4),这两个相位分布在每次迭代中,对目标图像的迭代估计进行修改。它保证算法收敛速度更快和相位掩码更加一致。

在一般情况下,定义上收敛准则可以是MSE的相关系数之间的重复和目标图像,如下

$$\text{MSK}(k) = \frac{1}{M * N} \sum_{m=1}^M \sum_{n=1}^N [|f(m, n)|^2 - |f_k(m, n)|^2]^2 \quad (5)$$

或

保留了传统的迭代算法^[11],也就是说,最终分阶段掩码Istrubutions确定它们的初始化。因此,FOPT(X, Y)和WOPT(U, V)的不同初始化将导致不同分布,如果键不匹配目标图像不能被解密,也就是说,来自迭代过程的密钥生成不同。

在实际系统中,掩码阶段量化有限的水平可能会降低解空间,并在恢复图像中引入噪声。为了弥补损失的质量,目标图像可以编码成相位掩码提供额外的寻找解

决方案的自由,这意味着图像加密与多阶段(级联)相关器^[12]。从安全的观点来看,这一战略显著地扩大了密钥空间(因为更多的密钥生成),使入侵更加困难。一般来说,被定义为 T - 阶段相关

$$f(x,y) = \text{IFT} \left\{ \text{FT} \left\{ \dots \text{IFT} \left\{ \text{FT} \{ \exp [i2\pi \varnothing^{(1)}(x,y)] \} \dots \right\} * \exp [i2\pi \varphi^{(2)}(u,v)] \right\} \dots \right\} \exp [i2\pi \varnothing^{(t-1)}(x,y)] * \exp [i2\pi \varphi^{(t)}(u,v)] \right\} \quad (7)$$

或

$$\hat{f}(x,y) = \text{IFT} \left\{ \text{FT} \left\{ \dots \text{IFT} \left\{ \text{FT} \{ I(x,y) \} * \exp [i2\pi \varphi^{(1)}(u,v)] \right\} \dots \right\} \exp [i2\pi \varnothing^{(t-1)}(x,y)] * \exp [i2\pi \varphi^{(t)}(u,v)] \right\} \quad (8)$$

因为 t 是奇数,矩阵 $I(x,y)$ 表示输入的平面波,下标 $i(i=1,2,\dots,t)$ 表示系统中掩码的序列号。这些掩码相位的分布可以推断式类比分析公式(3)。

2 计算机模拟

下面通过用数值模拟演示总体思路,目标图像的大小为 $205 * 128$ 与 256 级灰度图(如图 2)。目标图像两个阶段的掩码的大小相同,假设的光学系统是由平面波的幅度等同于 1 照亮,两种相位掩码随机初始化算法开始。接着阶段函数,通过向前和向后交替转换相关式定义式(1)~式(4),大约 3 次迭代后其相关系数达到 0.99,然后保持缓慢增加最终达到 1 次进行 20 次迭代之内,相应地检索图像的强度分布与目标图像是非常接近的。严格的说,相关系数收敛,但不等于 1,无论算法运行多少次迭代,因为式(1)没有分析解决方案可以找到,在这里它达到 1 只是因为两个图像之间的差异超出了数字计算机代表的精度。其实,CIFT 算法保留了传统的 POCS 算法误差降低的属性,MSE 的不断削减直到到达最低。CIFT 算法一个有趣特点是任意初始化过程可生成质量几乎相同的恢复图像,结果中的掩码分布不同(如图 3),因此优化阶段的掩码可作为安全系统关键,只有两个相位掩码,并分别与位于适当的平面 4-F 架构相互匹配,可以恢复目标图像。否则,输出是没有意义的。另一方面,密钥 $\exp[i2\pi\varphi(X,Y)]$ 和 $\exp[i2\pi\varphi(U,V)]$ 只有相位函数,并具有类似的随机分布,因为它提供防伪属性,所以这些字符可能会引入一个较高的安全级别(如图 4)。CIFT 算法另一个安全优势发生在真伪验证的应用,代替一个单一相关峰值检

测,验证系统依据 CIFT 算法检测一个重要的输出,以确定是否要验证输入。因此,不可能通过直接照射输出平面而绕过相关器引起虚假鉴定,因为入侵者在输出不正确的相位分布无法生成相同的图案。为安全起见,两个掩码需要分配给不同的两个人,只有在他们共同的授权下才能进行验证,而更高的安全性是必须检索到更多的相位掩码并分配给多个机构,以便减少密钥被盗的风险。



图 2 测试图像原图



图 3 不同算法相应的 100 次迭代输出图

	ψ_1	ψ_2	ψ_3
ϕ_1			
ϕ_2			
ϕ_3			

图 4 交叉相关性函数 $f(x,y)$ 和 $y(u,v)$ 在同一迭代过程可以恢复的目标图像

与以往的方法进行比较,CIFT 算法和以前的方法是相同的初始条件下的考察。分别设算法 A,B,C 和 D 表示前文中提出的方法。在文中提出的算法,算法 A 和 B 只是修改单一的掩码,分别位于傅里叶平面分布或输入平面,而 C 和 D 采用一种迭代过程修改两个掩码的分布策略。图 3(a)~(d) 显示这 4 种算法在 100 次迭代时图像相应的恢复。它表明,图 3(c) 和图 3(d) 比图 3(a) 和图 3(b) 具有更高的质量。导致这一事实可能有两个原因。首先,C 和 D 的解空间是显著扩大,因此它可能找到更好的解决方案。第二,后两种算法根据检索到的图像在目前迭代修改两个掩码的相位分布,这种策略保证了更好的解决方案和更快的收敛。然而,C 和 D 之间仍然是差别不大,算法 C 在输入和傅里叶平面交替修改相位分布。也就是说,它在第一阶段的某些

迭代检索掩码,同时固定其他,然后在下次迭代检索第二个,然后再检索第一个,这个循环不断直到算法收敛。但它不是这种情况下提出的算法,在每个迭代同步修改两个阶段,这种变化会导致更快的收敛速度和较高的恢复质量。四个算法的目标图像以及所述迭代图像之间的均方误差和相关系数,分别由式(5)和式(6)定义。表1所示A及B分别是在100次迭代的效果,显然结果与图3得到的是一致的。需要指出的是,虽然图3(c)和图2、图3(d)和图2之间的相关系数似乎都等于1,但其对应的MSE有很大的不同。如表1显示CIFT算法得到的迭代图像质量显著高于其他方法,得到最好的最有效搜索策略。

表1 四种算法在100次迭代下均方误差与相关系数的比较

Algorithm	A	B	C	CIFT
MSE	0.006 2	0.001 77	4.354×10^{-11}	$1.086 7 \times 10^{-18}$
R	0.987 1	0.996 4	1.0	1.0

评估收敛,设置的趋同标准 $R = 0.988$ 。这些算法都在相同初始条件下测试。在这个模拟中,算法A需要124.63 s和632次迭代,算法B需要25.72 s和100次迭代,算法C需要3.97 s和15次迭代,分别驱动R这个临界值。相对而言,达到同样的阈值CIFT算法只需要2.358 s和9次迭代。显然,作为在前文的评论,C和D有更快的收敛速度。相应的算法的MSE如下:算法A为 $9.834 5 \times 10^{-4}$, 算法B为 1.7×10^{-3} , 算法C为 1.3×10^{-3} ,CIFT算法为 $6.456 2 \times 10^{-4}$ 。然而,如果迭代过程继续进行,直到MSE不再有任何减少,这个值则是完全不同的。

3 结束语

文中提出级联迭代傅里叶变换(CIFT)算法在光学安全应用相位掩模的设计。CIFT算法与以往的方法相比,调整了两个相位掩码同步分布以及扩大搜索空间,

因此有更快的收敛速度和更好的恢复图像的质量。该算法分为两个阶段掩码,作为安全系统密钥编码目标图像,这些密钥被分配到不同的人能获得较高的安全水平。

参考文献:

[1] 王永瑛. 基于计算全息和迭代傅里叶变换算法的光学图像加密技术的研究[D]. 济南:山东大学,2007.

[2] 乌 旭. 基于随机相位编码的加密与防伪技术研究[D]. 大连:大连理工大学,2006.

[3] 丛长平. 信息安全中的光学加密及数字水印技术[D]. 大连:大连理工大学,2009.

[4] 王永瑛,王玉荣,杨永斌. 用迭代傅里叶变换算法实现光学分级图像加密[J]. 中国激光,2006,33(10):1360-1364.

[5] 赫明钊,曹良才,谭峭峰. 基于级联分数傅里叶变换系统的数字水印技术[J]. 光学学报,2009,29(10):2709-2715.

[6] 贾丽娟,刘正君. 基于随机分数傅里叶变换的双图像加密算法[J]. 光子学报,2009,38(4):1020-1024.

[7] 吴克难,胡家升,乌 旭. 信息安全中的光学加密技术[J]. 激光与光电子学进展,2008,45(7):30-38.

[8] Réfrégier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding[J]. Optics letter, 1995,20(7):767-769.

[9] Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain[J]. Optics letter,2000,25(12):887-889.

[10] Javidi B, Horner J L. Optical pattern recognition for validation and security verification[J]. Optical engineering,1994,33(6):1752-1756.

[11] Javidi B, Sergeant A. Fully phase encoded key and biometrics for security verification[J]. Optical engineering,1997,36(3):935-942.

[12] Weber D, Trolinger J. Novel implementation of nonlinear joint transform correlators in optical security and validation[J]. Optical engineering,1999,38:62-68.

+++++ (上接第167页)

术,2005,28(8):91-93.

[4] 李金良. 智能卡操作系统(COS)编程语言及编译器系统设计与实现[J]. 中国集成电路,2005(11):67-69.

[5] 李 翔. 智能卡研发技术与工程实践[M]. 北京:人民邮电出版社,2003.

[6] 张志刚,赵 奎. 智能卡操作系统研究和实例分析[J]. 企业技术开发,2005,24(9):18-20.

[7] ISO 7816-3. Identification cards integrated circuit(s) cards with contacts-Part 3:Electronic signals and transmission protocols[S]. [s.l.]:International Electrotechnical Commission, 1997.

[8] 张利华. 智能卡操作系统开发中的测试技术[J]. 计算机工程与设计,2004,25(6):901-902.

[9] GB/T20276-2006. 信息安全技术智能卡嵌入式软件安全技术要求(EAL4 增强级)[S]. 2006.

[10] CCDB-2010-03-001. Smartcard evaluation[S]. 2010.

[11] Common methodology for information technology security evaluation[S]. 2009.

[12] CCDB-2009-03-001. Application of attack potential to smartcards[S]. 2009.

基于级联迭代傅里叶变换算法的光学安全技术

作者：[容强, RONG Qiang](#)

作者单位：[郑州轻工业学院 易斯顿美院, 河南 郑州, 451450](#)

刊名：[计算机技术与发展](#)

英文刊名：

Computer Technology and Development

ISTIC

年, 卷(期):

2014(2)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjfz201402042.aspx