文章编号:1004-4213(2010)07-1263-5

基于公匙密匙分配体制的光学加密系统*

邓晓鹏

(怀化学院 物理与信息工程系,湖南 怀化 418008)

摘 要:针对光学变换加密系统的密匙安全管理和分发问题,提出了基于公匙密匙分配体制和光学变换的混合加密系统.首先利用光学加密系统对原始图像进行加密,然后对光学加密系统的工作密匙进行压缩,最后利用公匙密匙分配体制对压缩后的密匙进行分配和管理.解密时,接收方不需要等待,就可以预先利用公匙密匙分配体制获得解密密匙.理论分析和仿真实验表明,该方法不仅充分利用了光学变换加密系统具有多重密匙的特点,解决了密匙的安全分配和管理问题,而且突出了混合加密系统的速度优势.

关键词:信息光学;图像加密;公匙密匙分配体制; 光学变换

中图分类号:0438 **文献标识码**:A **doi**:10.3788/gzxb20103907.1263

0 引言

信息社会中,信息安全成为一个值得关注的课题,由于它在很多领域中可以减少巨大的经济损失,因此在学术和产业界引起了极大的兴趣.由于光学图像加密技术存在许多明显的如高速并行运算、多个加密自由度、高安全性能等优点,近年来,人们提出许多利用光学方法进行图像加密的技术[1-6].在这些方法中,为了进一步提高加密系统的安全性能,往往采用加密自由度比较多的系统,如扩展分数傅里叶变换系统、分数傅里叶变换系统、菲涅耳衍射系统等[3-5].但是,由于这些系统均属于对称加密系统,系统的安全性能完全依赖于密匙的秘密性,密匙的安全分发和管理成为这类加密系统的一个致命弱点.针对这个问题,一些学者提出一种基于公匙密码体制的光学混合加密技术[7-8],在该技术中,先利用传统的光学系统对原图像进行加密,然后利用公匙密码体制对系统密匙(工作密匙)进行加密,实现系统密匙的安全分发.但是,对于靠增加密匙长度来提高安全性能的光学加密系统来说,由于公匙密匙加密系统的最大缺点就是实现速度远不如对称密匙加密系统,因此,采用公匙密码体制对长度比较长的工作密匙进行加解密速度非常慢,而且解密方要想利用公匙密码体制获得工作密匙,必须等待加密方传送加密的工作密匙,从而造成整个混合加密系统的效率非常低,因此,该技术虽然解决了密匙分配和管理问题,但是并没有显示出这种混合加密系统在速度上的优势,而且加密后不仅要向接收方传输加密图像,还要传输加密后的工作密匙.基于上述加密系统的缺陷,本文提出一种基于公匙密匙分配体制和光学变换的混合加密系统.在该技术中,首先利用光学加密系统对原始图像进行加密,然后对光学系统的工作密匙进行压缩,最后利用公匙密匙分配体制对压缩后的密匙进行分配和管理.这样既充分利用了光学变换具有多重密匙的特点,解决了密匙的安全分配和管理问题,又突出了混合加密系统的速度优势,而且不需要传送加密的工作密匙.

1 基于光学变换的双相位序列加密系统

在现有的光学加密系统中,大部分是基于某种光学变换而实现的,具体系统模型如图 1.

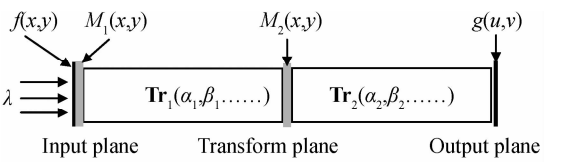

图 1 基于光学变换的加解密系统模型

Fig. 1 The encryption/decryption system model based on optical transform

其中 λ 为照射光波长,α_i,β_i……为光学变换系统参量,(x,y)、(x',y')和(u,v)分别为输入面、变换面和输出面的坐标.在加密阶段,待加密图像 $f(x,y)$在输入面与相位掩模 $M_1(x,y)$相乘,然后通过光学变换 $\mathbf{Tr}_1$,在变换域与相位掩模 $M_2(x',y')$相乘,再通过光学变换 $\mathbf{Tr}_2$,最后在输出面得到加密图像 g

*湖南省教育厅科研项目(07C506)和怀化学院科研项目资助

Tel:0745-6630171 Email:dxpzqh@163.com

收稿日期:2009-10-13 修回日期:2009-11-07

(u,v). 整个加密过程可用式(1)表示为

$$g(u,v)=\mathbf{Tr}_2\{\mathbf{Tr}_1[f(x,y)\cdot M_1(x,y);\lambda,\alpha_1,\beta_1\cdots\cdots]\cdot M_2(x',y');\lambda,\alpha_2,\beta_2\cdots\cdots\} \quad (1)$$

从上述加密过程可以看出，波长 λ、变换系统参量 α_1、β_1……、α_2、β_2……以及 $M_1(x,y)$ 和 $M_2(x',y')$一起为密匙设计提供了巨大的空间. 解密时，缺少其中任何一个都不能恢复原图像，密匙空间非常大，系统安全性能非常高[3-6]. 因此，从安全角度来衡量，这样的加密系统是最优的. 但是由于该系统在加密和解密时使用是相同的密匙，因此它仍然属于对称加密系统，系统的安全性能完全依赖于密匙的安全性，为了保证密匙的安全分配和管理必须采取其他办法. 如果又采取对称加密技术对密匙进行加密传送，将会陷入无休止恶性循环，显然是不现实的. 为了解决这个问题，一些学者提出一种基于公匙密码体制的光学混合加密技术[7-8]，先利用传统的光学变换系统对原图像进行加密，然后利用公匙密码体制对系统密匙(工作密匙)进行加密，从而实现系统密匙的安全分发. 虽然公匙密匙加密系统对于安全通信似乎是理想的，但是它的最大缺点就是加解密速度远不如对称密匙加密系统，因此采用公匙密码体制对长度比较大的工作密匙(如相位掩模)进行加解密速度非常慢，而且解密方要等到接收到加密的工作密匙后，才能对它进行解密获得工作密匙，从而造成整个混合加密系统的加密效率非常低，因此，该技术虽然解决了密匙分配和管理问题，但是并没有显示出速度的优势.

2 基于公匙密匙分配体制和光学变换的混合加密系统

针对加密技术的缺陷，在综合考虑系统安全和速度的基础上，提出一种基于公匙密匙分配体制和光学变换的混合加密系统. 与基于公匙密码体制的光学混合加密系统不同的是[7-8]，不是直接利用公匙密码体制对光学系统的工作密匙逐个进行加密，而是先对光学系统的工作密匙进行压缩，然后利用公匙密匙分配体制对压缩后的工作密匙进行分配和管理. 这样将大大增强系统的效率.

在光学加密系统的工作密匙中，相位掩模的长度是最长的，为了节省时间，在利用公匙密匙分配体制对它进行分配之前，必须对它进行压缩处理. 在常用的相位掩模中[9-10]，虽然随机相位序列具有极高的安全性能，但是由于序列中的元素具有完全随机性的特点，因此不能用一个确定的数学方程或公式进行重构，而混沌序列的类随机性和确定性特点，既保证了极高的安全性能又能利用非线性叠代方程进行重构，对于特定的非线性叠代方程，只要控制初始值，便可控制整个序列[9]，因此用混沌序列来构造相位掩摸便于重构和压缩. 另外，系统的其他工作密匙 α_1、β_1……、α_2、β_2……也可以令它们为混沌序列某一位置的元素，对于那些系统工作密匙中还包括波长和焦距的变换系统，如广义分数傅里叶变换系统，由于波长和焦距的具体大小不能为任意值，供它选择的数值范围有限，因此把它们作为公共参量，对系统安全影响不大. 这样，光学加密系统中的所有的工作密匙，除了波长和焦距以外，均可由一混沌序列来确定. 解密时仅用相应的初始条件从确定性系统获得浑沌序列重构相位阵列和其他系统参量即可获得工作密匙. 对于上述系统，由于原来的工作密匙已被压缩到只有一个，即混沌序列的初始值，因此这个初始值对系统的安全显的至关重要. 为了保证对它进行安全分发和管理，我们利用公匙密匙分配体制对它进行分配. 本文所采用公匙密匙分配体制是由美国学者 Diffie-hellman 提出的，它的理论基础是有限域上指数函数的单调性，即计算有限域上的指数很容易，但是计算有限域上对数的整数解很困难. 具体分析如下：设 q 为素数，则在具有 q 个元素的有限域上的指数可以表示为

$$y\equiv g^x \pmod q \qquad (1\leqslant x\leqslant q-1) \quad (2)$$

式中 g 为有限域上的原根，且 $1<g<q$，x 分布在有限域上的所有非零整数元素集上. 当 q 为素数时，y 也是分布在有限域上的所有非零整数元素集上. 从式(2)不难推知，x 可以表示为在有限域上以 g 为底 y 的对数，即

$$x\equiv\log_g y \pmod q \qquad (1\leqslant x\leqslant q-1) \quad (3)$$

根据式(2)，已知 x 计算 y 十分容易，但是已知 y 利用式(3)计算 x 却极其困难. Diffie-hellman 密匙分配体正是利用这种单向性构成的. 在具体用它进行密匙分配时，其协议如下：系统中的每一个用户都从整数集$\{1,2,3,q-1\}$上随机选择一个数作为自己的私密密匙. 例如用户 A 和 B 选择的私密密匙分别记为 x_a 和 x_b. 然后根据式(2)计算出 y_a 和 y_b 为

$$y_a\equiv g^{x_a} \pmod q \quad (4)$$

$$y_b\equiv g^{x_b} \pmod q \quad (5)$$

式中 q、g 均为 Diffie-hellman 体制已知的公共参量. 用户 A 和 B 分别将 y_a 和 y_b 作为自己的公开密匙，连同自己的姓名、地址一起放到系统的用户公开密匙簿中. 当双方需要通信时，通过式(6)

$$K_{ab}=y_b^{x_a}=y_a^{x_b}=g^{x_a x_b} \pmod q \quad (6)$$

即可获得工作密匙，计算速度非常快，易于实现，但是在不知私匙的情况下，却十分困难.

根据上述公匙密匙分配体制，在加密前，通信双

方根据式(6)获得混沌序列的初始值.考虑到式(6)中的 k_{ab} 是一个在 1 到 $q-1$ 范围内的整数,而混沌序列均为 0 到 1 范围内的小数,因此令混沌序列的初始值为

$$x_0 = k_{ab}/(q-1) \tag{7}$$

然后利用式(8)所表示的非线性叠代方程获得混沌序列$\{x_k : k=0,1,2,3\cdots\cdots n\}$.

$$x_{k+1} = \gamma x_k(1-x_k) \tag{8}$$

式中 γ 为控制参量.对于上述叠代方程,当控制参量取值在 $3.569<\gamma<4.000$ 范围内时,迭代结果出现了混沌现象,且 x_k 为 0 到 1 范围内混沌序列.如果原始图像大小为 $M\times N$,则在混沌序列 x_k 中选取 $2M\times 2N+n$(n 为系统参量的总个数)个元素构成光系统的加密密匙对原始图像进行加密.接收方按照同样的方法获得解密匙对加密图像进行解密.具体加解密方框图如图 2.

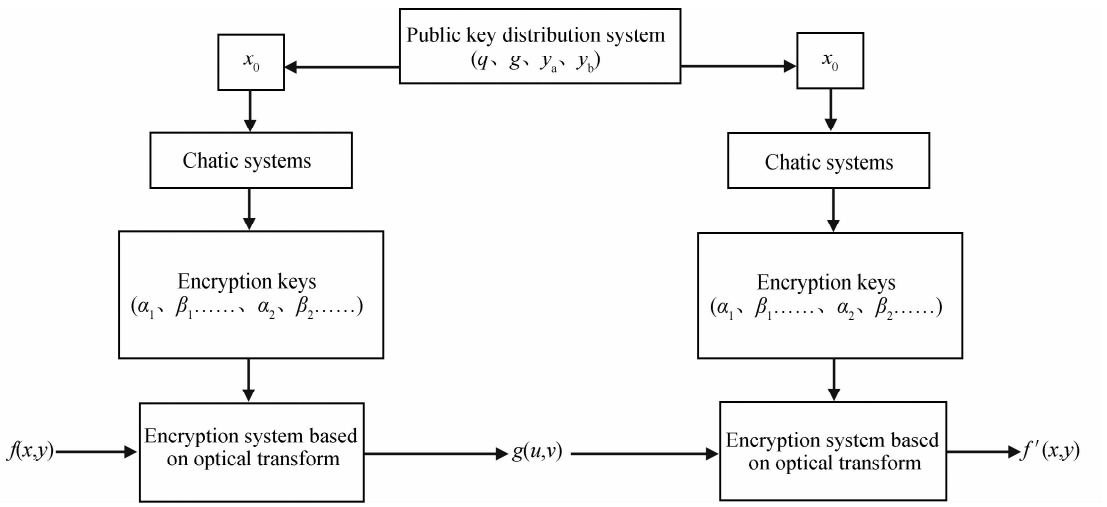

图 2　基于公匙密匙分配体制的加解密方框图

Fig. 2　Block diagram for encryption and decryption based on public key distribution system

3　实验仿真

为了验证方法的可行性,以广义分数傅里叶变换系统作为加密系统为例,利用 Matlab 进行了仿真实验.实验时,公匙密匙分配体制中的公共参量 g 为 3,q 为 524 287(越大保密强度越高,由于普通电脑的运算准确度只有 15 位,所以取的比较小),私密密匙 x_a 为 29,x_b 为 33,然后根据式(4)和(5)得到公开密匙 $y_a=59\ 601$,$y_b=65\ 358$,并把它们和公共参量、姓名、地址一起放到系统的用户公开密匙本中.加密方利用自己的私密密匙 x_a 和系统参量以及公开密匙 y_b 根据式(6)得到 $K_{ab}=387\ 606$,然后利用式(7)获得混沌序列的初始值 $x_0=387\ 606/524\ 286$ 并生成混沌序列,其中 γ 取 3.689.为了确保越过瞬态过程,在记录序列之前先摔掉前 400 位,同时考虑到此时的系统参量 α_1、β_1、α_2、β_2(分别为输入和输出面离透镜的距离且以米为单位)和相位掩模实际制造的精确度,利用四舍五入只取到小数点后两位.图 3(a)是以 $x_0=387\ 606/524\ 287$ 作为初始值生成的混沌序列 A;图 3(b)是以 $x_0=387\ 605/524\ 286$ 作为初始值生成的混沌序列 B;图 3(c)是它们的差值 $A-B$.

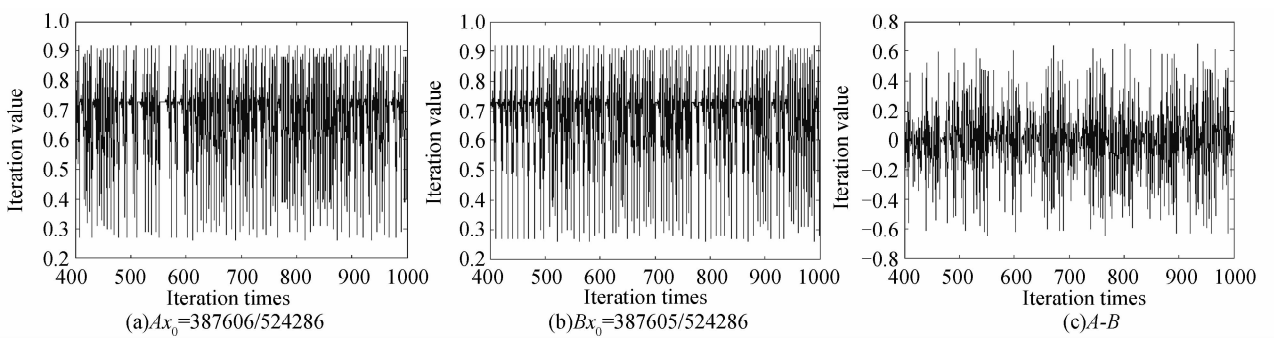

图 3　不同初始值的混沌序列及其差值

Fig. 3　Chaotic sequence with different initial parameter and their difference

从上图可以看出，虽然我们只取到小数点后两位，但是两者差别非常很大，因此抗攻击能力非常强. 选取混沌序列的第 k 到 $k+3$ 位元素 0.77 0.64 0.83 0.51 分别为 α_1、β_1、α_2、β_2，第 $k+4$ 到 $k+3+M*N$ 位元素生成相位掩模 M_1，第 $k+4+M*N$ 到 $k+3+2M*N$ 位元素生成相位掩模 M_2（在这里 k 取 401，M 和 N 均取 128）. 图 4(b)和 4(c)分别是 M_1 和 M_2 的实部分布，图 4(d)是最后的加密图像，其中照射光波长为 632.8 nm，透镜焦距分别为 30 cm 和 40 cm. 接收方接收到加密图像后，利用自己的私密密匙 x_a 和系统参量以及公开密匙 y_a 根据式(6)得到 $K_{ab}=387\ 606$，然后按照同样的方法获得解密密匙. 图 4(e)是利用正确密匙的解密图像，图 4(f)是错误密匙的解密图像（$K_{ab}=387\ 605$）.

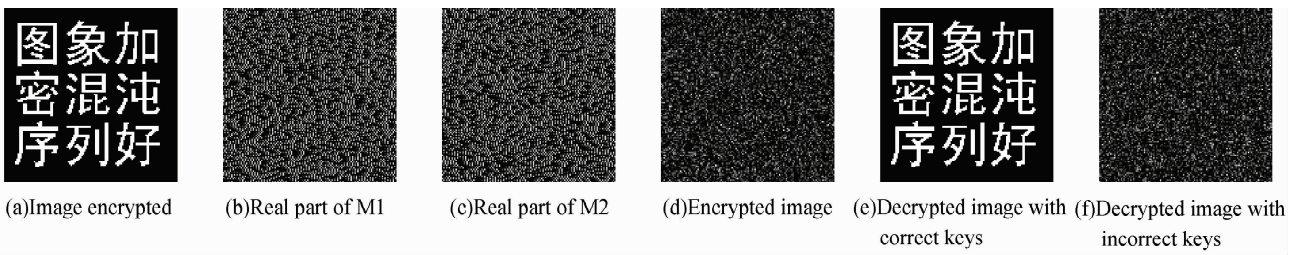

图 4 仿真实验结果

Fig. 4 Simulated results

4 系统效率和安全性能分析

从加解密原理和仿真过程来看，利用公匙密匙分配体制对光学系统工作密匙进行分发，不像文献中所叙述的那样，加密方先利用公匙密码体制对光学系统工作密匙特别是相位掩模中的元素逐个进行加密，并通过特定的通道进行传送，然后接收方接收到加密工作密匙并利用公匙密码体制解密光学系统的工作密匙[8]. 公匙密匙分配体制是把光学系统中所有工作密匙作为一个整体进行分发，只要通信双方按照事先约定好的公共参量，不需要通过任何通道进行传送，便可获得光学加密系统的密匙，即接收方不需要等待，就可以预先获得光学系统的解密密匙，克服了公匙密码体制速度慢过程复杂的缺点，大大增强了混合加密系统的效率.

对于系统的安全性能，首先，根据 Diffie-hellman 体制的原理，其保密性强烈地依赖于模数 q 的大小，为了提高保密强度，可以选择足够大的模数，如 100 位. 如果破解一次所需要的时间为1 min，可以粗略估计出采用穷举法破解的整个时间大约为 94 年，况且破解一次的时间再加上利用光学方法进行验证的时间大大超过 1 min，因此就 Diffie-hellman 体制的设计原理来说，系统是足够安全的. 另外，在选取混沌序列作为工作密匙时，虽然进行了四舍五入，只取到小数点后两位，但是由于混沌序列对初始值高度依赖性，保证了所选取的密匙因初始值的细微差别而截然不同，这样并不会降低穷举法攻击的难度.

5 结论

本文在回顾现有光学图像加密技术的基础上，首先分析它们存在的缺陷及其产生的原因，然后提出了基于公匙密匙分配体制的光学加密技术，最后对该技术的有效性和可行性进行了仿真实验. 理论分析和仿真实验表明，利用公匙密匙分配体制对光学变换加密系统的密匙进行分配和管理完全是可行的，该方法不仅充分利用了光学变换加密系统具有多重密匙的特点，解决了密匙的安全分配和管理问题，而且突出了混合加密系统的速度优势.

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] SITU G, ZHANG J. Multiple-image encryption by wavelength multiplexing[J]. *Opt Lett*, 2005, **30**(11): 1306-1308.

[3] SITU Guo-hai, ZHANG Jing-jua. Double random-phase encoding in the Fresnel domain[J]. *Opt Lett*, 2004, **29**(14): 1584-1586.

[4] HENNELLY B, SHERIDAN J T. Optical image encryption by random shifting in fractional Fourier domains[J]. *Opt Lett*, 2003, **28**(4): 269-271.

[5] NISHCHAL N K, JOSEPH J, SIGNH K. Optical encryption using cascaded extended fractional Fourier transform[J]. *Opt Mem Neural Net*, 2003, **12**(2): 139-145.

[6] WANG Hong-xia, ZHAO Wei. Six security key for image encryption based on anamorphic fractional fourier transform [J]. *Acta Photonica Sinica*, 2007, **36**(4): 759-762.
王红霞，赵玮. 基于变形分数傅里叶变换的六重密钥图像加密[J]. 光子学报，2007，**36**(4)：759-762.

[7] PENG Xiang, ZHANG Peng. Vitural-Optical information security system based on public key infrastructure[C]. *SPIE*, 2005, **5642**: 52-60.

[8] LIN G S, CHANG H T, LIE W N. Public-key-based optical image cryptosystem based on data embedding techniques [J]. *Opt Eng*, 2003, **42**(28): 2331-2339.

[9] ZHANG Pei-kun, LI Yu-lin. Optical image encryption & decryption using chaotic sequence to construct the phase array [J]. *Acta Photonica Sinica*, 1998, **27**(11): 979-982.
张培琨，李育林. 用浑沌序列构造相位列阵加密和解密光学图

象[J]. 光子学报,1998,**27**(11):979-982.
[10] BARRERA J F, HENAO R H, TORROBA RD. Optical encryption method using zone plates[C]. *SPIE*, 2004, **5622**: 1129-1132.

Optical Encryption Based on Public Key Distribution System

DENG Xiao-peng
(*Department of Physics and Information Engineering, University of Huaihua, Huaihua, Hunan* 418008, *China*)

Abstract: A hybrid encryption in the optical transform domain based on public key distribution system is proposed aiming at safely deliver and management of optical encrypted system. Frist, the original image is encrypted based on optical system, and then, the work key of optical system is compressed, finally, distribution and management of the compressed key is dong by public key distribution system. In the decryption stages, the receiver do not need to wait and can obtain dencryption key in advance by means of public key distribution system. The theoretical analysis and computer simulation results show that the proposed method can solve the problem of safely deliver and management and make good use of multi-dimensional keys that encrypted system of optical transform possess. Also, this method highlight advantage of hybrid system speed.

Key words: Information optics; Image encryption; Public key distribution system; Optical transform

DENG Xiao-peng was born in 1972. He received the M. S. degree from University of Electronic Science and Technology of China in 2006. Now he is an associate professor and works at Huaihua University, and his major research interests focus on optics information process.