

基于分频域相位和幅度的数字图像加密新方法

王银花, 王丽萍

(铜陵学院 电气工程系, 安徽 铜陵 244000)

摘要:伴随着网络技术和多媒体技术的飞速发展,多媒体数据逐渐成为人们获取信息的重要来源,并成为人们生活的重要组成部分。因而,如何保护多媒体信息的安全成为国际上研究的热门课题。文中提出利用混沌序列实现对图像分数傅里叶系数矩阵的加密,为图像加密提供了一个新方案。实践表明,该方法具有密图文件保密性高、密钥简单等特点。

关键词:数字图像;分数傅里叶变换;图像加密

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2009)04-0177-03

A New Image Encryption Method Based on Phase and Amplitude of Fractional Domain

WANG Yin-hua, WANG Li-ping

(Department of Electrical Engineering, Tongling College, Tongling 244000, China)

Abstract: The digital media has become a main way for information communication along with the wide use of network. At the same time, multimedia information security problems including copyrights piracy emerged as side effects of the popularity of digital representation and distribution over network. In this paper, the discrete fractional Fourier transform coefficient matrix was transformed by chaotic sequences. It points out a new method of image encryption. The test results show that the new encryption method will keep the image file in high secrecy and the key is simple.

Key words: digital image; fractional Fourier transform; image encryption

0 引言

随着网络技术的飞速发展,大量的图像数据开始在网上进行传输和交流。在互联网上传输的图像数据有很多是要求发送方和接受方要进行保密通信,如军用卫星所拍摄的图片、军用设施图纸、新型武器图、金融机构的建筑图纸等。这些图像信息不但涉及个人隐私,而且有些涉及到国家安全,因而图像数据的保护越来越受到社会的普遍重视。

数字图像加密源于早期的经典加密理论,其目的是将一幅给定的图像按一定的变换规则在空间域或频域将其变换为一幅杂乱无章的图像,从而隐藏其图像本身的真实信息。加密方法可分为空间域算法和频域算法。空间域算法的优点是实现简单,且加密过程中不会引入额外的图像畸变,但加密强度不够^[1~3]。相对于空间域算法,频域算法加密效率较高,由于在变

换中可设置不同的参数和采用算法复杂度高的算法,可保证图像信息有较高的安全性^[4~6]。

文中提出对数字图像进行分数傅里叶变换,然后对其相位谱和幅度谱用映射生成的混沌序列进行置乱的方法,可获得安全度较高的加密图像。

1 理论基础

1.1 分数傅里叶变换的定义及相关的基本性质

分数傅里叶变换作为一种新的信号表征方式,已经在信息加密、信息隐藏、模式识别等领域得到了广泛的应用。设输入信号为 $f(x)$, 则一维函数(将自变量改为二维矢量就可以直接推广到二维情况)的 p 阶分数傅里叶变换定义为^[7]:

$$f_p(x_p) = C_p \times \exp(j\pi \frac{x_p^2}{\tan\phi}) \times \int_{-\infty}^{+\infty} f(x) \times \exp(-j\pi \frac{x^2}{\tan\phi}) \times \exp(-2j\pi \frac{xx_p}{\sin\phi}) dx \quad (1)$$

其中常数

$$C_p = \frac{\exp\{-j[\pi \operatorname{sgn}(\sin\phi)/4 - \phi/2]\}}{\sqrt{|\sin\phi|}} \quad (2)$$

收稿日期:2008-07-14

基金项目:安徽省高校青年教师资助项目(2008jq1141);铜陵学院自然科学研究项目(2007tlxykj004)

作者简介:王银花(1977-),女,安徽巢湖人,讲师,硕士,研究方向为图像加密与水印;王丽萍,副教授,主要从事信息安全工作研究。

$p(0 < |p| < 2)$ 为分数阶, $\phi = p \cdot \frac{\pi}{2}$ 。

特别的, 当 $p = 1$ 时, 上式分数傅里叶变换即为普通傅里叶变换。

由此定义可得出分数傅里叶变换的两条重要性质:

(1) 可加性: $f_{p1}(f_{p2}) = f_{p1+p2}$;

(2) 周期性: 当 $p1 + p2 = 4n$ 时, $f_{p1+p2} = f$, 其中 n 为整数。

1.2 混沌序列定义及其在文中的应用

1.2.1 混沌序列定义

由于混沌理论是动力系统从有序突然变为无序状态的一种演化理论, 如果给定一个离散混沌系统两个非常接近的初始值, 则经过几次迭代后, 输出的结果可以完全不相关, 因此利用混沌系统对初始条件极其敏感的依赖性, 可以提供数量众多、非相关、类随机而又可确定可再生的混沌序列, 其非常大的周期性和优良的随机性, 不仅非常适合产生符合安全要求的序列密码, 而且可以提供数量众多的密钥。

一类非常简单却被广泛研究的动力系统是 logistic 映射, 其定义如下^[8]:

$$x_{k+1} = \mu x_k (1 - x_k) \quad (3)$$

其中, $0 \leq \mu \leq 4$ 称为分枝参数, $x_k \in (0, 1)$ 定义同上。混沌动力系统的研究工作指出, 当 $3.5699456 \dots < \mu \leq 4$ 时, logistic 映射工作于混沌态。也就是说, 由初始条件 x_0 在 logistic 映射的作用下所产生的序列 $\{x_k; k = 0, 1, 2, 3 \dots\}$ 是非周期的、不收敛的并对初始值非常敏感。

另一类简单的映射是 Chebyshev 映射, 以阶数为参数。k 阶 Chebyshev 映射定义如下:

$$\tau(x_{k+1}) = \cos(n(\arccos x_k)) \quad (4)$$

其中 x_k 的定义区间是 $(-1, 1)$ 。事实是通过简单的变量代换, logistic 映射同样可以在区间 $(-1, 1)$ 上定义。其形式如下:

$$x_{k+1} = 1 - \lambda x_k^2 \quad (5)$$

其中 $\lambda \in [0, 2]$ 。在 $\lambda = 2$ 的满射条件下, logistic 映射与 Chebyshev 映射是拓扑共轭的。

1.2.2 混沌序列在文中的应用

密码学中, 使用置换来进行数据变换, 主要有两种作用: 其一是对数据内容作不可预测的替换; 其二是改变数据在数据序列中的位置, 即随机换位。这里将混沌序列引入密码置换网络, 利用混沌映射产生序列的非线性以及其轨道点的遍历性, 来产生置换网络的双射变换所需地址。

设二维数据矩阵表示为 $A = [a_{i,j}]M \times N$, 其中

$a_{i,j}$ 代表第 i 行第 j 列像素的值。对 A 进行行列置乱处理。置换阵列的行地址和列地址由混沌序列产生。

2 加密/解密方法

设输入图像用 $f(x, y)$, 分数傅里叶变换记为 $F_{(px, py)}$, px, py 分别为 x, y 方向的分数傅里叶变换阶数。

对图像进行分数傅里叶变换, 得到:

$$G(\xi, \eta) = F_{(px, py)}\{f(x, y)\} = A(\xi, \eta) \exp[jB(\xi, \eta)]$$

式中 $A(\xi, \eta)$ 和 $B(\xi, \eta)$ 分别是分数傅里叶谱的振幅和相位成分。

根据系统加密的设计原则, 文中提出对图像进行分数傅里叶变换, 再对变换后的振幅谱或相位谱进行混沌置乱处理。图像加密主要步骤:

步骤 1: 对大小为 $M \times N$ 的任意图像, 作阶次为 (px, py) 的分数傅里叶变换。每一次变换都包含 x 和 y 两个方向, 即有 px, py 两个变换密钥。得到分数傅里叶变换系数矩阵。

步骤 2: 确定一维 Chebyshev 系统的初始参数。设用户密钥为 x_{01}, x_{02} 。利用密钥值 x_{01}, x_{02} 采用公式 (4) 生成实数值混沌序 x_{1k}, x_{2k} , 在该算法中不使用该序列的初始段部分, 设起始位置分别为 n_1, n_2 , 然后由 x_{1k} 和 x_{2k} 分别生成二维置换阵列的行地址和列地址, 这里采用两个 Chebyshev 映射产生的序列加 1 成为区间 $[0, 2]$ 间的数, 然后乘以 $(M+1)/2$ 和 $(N+1)/2$ 取整来作为置换阵列的行地址和列地址。密钥为 $(x_{01}, x_{02}, n_1, n_2)$ 。

步骤 3: 对得到的振幅谱或相位谱进行行列置乱。也可以对振幅谱和相位谱同时置乱, 密钥更安全。文中为介绍简单起见对得到振幅谱和相位谱矩阵分别加密。

解密过程为加密过程的逆。首先根据密钥生成逆置乱序列, 对加密的振幅谱或相位谱进行列逆置乱。再进行分数傅里叶反变换, 达到解密图像的目的。

3 仿真结果与分析

为了验证文中提出的加密算法, 在 MATLAB7.0 中实现图像分数傅里叶变换, 并做了相关实验。使用的原始图像为 256×256 的 256 灰度级标准“lena”图像。对加密图像进行了破解实验。图 1 为原始图像。图 2(a) 是对图 1 原始图像先进行分数傅里叶变换, 然后再对其振幅谱用混沌序列进行置乱得到加密图像。图 2(b) 是对图 1 原始图像先进行分数傅里叶变换, 然

后再对其相位谱用混沌序列进行置乱得到加密图像。两处的密钥均为:分数傅里叶变换阶数密钥(p_x, p_y) = (0.8, 0.9)、混沌系统控制参数密钥为(0.2, 0.6, 170, 160)。



图1 原始图像



图2 加密图像

对加密后的图像进行解密。图3(a)、(b)、(c)是对图2(a)的错误解密图像。其中图3(a)和(b)均为分数傅里叶变换密钥正确,置乱反变换密钥不正确得到的解密图像;图3(d)为分数傅里叶变换密钥不正确,置乱反变换密钥正确得到的解密图像。错误密钥分别是:(x_{01}, x_{02}, n_1, n_2) = (0.20000001, 0.6, 170, 160)、(x_{01}, x_{02}, n_1, n_2) = (0.2, 0.6, 170, 180)、(p_x, p_y) = (0.85, 0.95)。



图3 对图2(a)的错误解密图像



图4 对图2(b)的错误解密图像

图4(a)、(b)、(c)是对图2(b)的错误解密图像。其中图4(a)和(b)均为分数傅里叶变换密钥正确,置乱反变换密钥不正确得到的解密图像;图4(c)为分数

傅里叶变换密钥不正确,置乱反变换密钥正确得到的解密图像。错误密钥分别是:(x_{01}, x_{02}, n_1, n_2) = (0.2, 0.60000001, 170, 160)、(x_{01}, x_{02}, n_1, n_2) = (0.2, 0.6, 170, 180)、(p_x, p_y) = (0.82, 0.92)。

图5是密钥都正确时的解密图像。其中图5(a)是图2(a)的正确解密图像,图5(b)是图2(b)的正确解密图像。



图5 密钥都正确时的解密图像

大量实验表明,加密密钥中混沌序列的初始存在很小的偏差,图像解密将无法完成。当解密设置的混沌序列的起始位置与密钥起始位置接近时只能看到图像的小部分信息,而混沌序列的起始位置存在很大的密钥空间,可实现较高安全程度。当混沌密钥正确,而分数傅里叶变换密钥不正确也看不到清晰的图像。可见只有同时知道置乱密钥和分数傅里叶变换密钥时才能得到原始图像信息。

4 结束语

给出了一种简单有效的图像加密方法,通过对数字图像进行一定阶次的分数傅里叶变换,然后用二维混沌置乱网格来加密变换后的振幅谱和相位谱。通过仿真实验结果,可充分证明文中提出的方法具有很好的安全性,具有密图文件保密性高,密钥简单,重构图像与原图像一致性良好等特点。

参考文献:

- [1] 陈永强,孙华宁.基于二维混沌映射的数字图像加密算法[J].武汉工业学院学报,2004,23(4):45-47.
- [2] 叶永伟,杨庆华,王颖玉.用混沌序列对数字图像进行魔方加密[J].浙江工业大学学报,2003,32(2):173-176.
- [3] 罗维潮,付永庆.一种基于小波变换的二维Logistic混沌图像加密算法[J].黑龙江工程学院学报:自然科学版,2007,21(2):41-44.
- [4] 陈帅,钟先信,朱士永,等.基于线性同余的伪随机序列图像加密[J].计算机技术与发展,2006,16(4):23-24.

(下转第183页)

体集合的交互和访问功能,为了实现系统中各客体基于部门级权限的访问控制,系统采用了部门——客体映射机制,将所有客体划分各部门中,另外在实现中还可能存在如下问题:①部分客体可能同时归属多个部门,因此访问时可能造成资源调度冲突;②客体来源于系统之外,具有一定的不确定性,所以各客体标识可能与系统标识发生冲突或者客体标识规范与应用系统不一致,为此文中采取系统内映射的方式来解决上述问题,即系统使用的所有客体都需要在本系统中注册成为内部应用分配唯一编码,并归属各部门统一调配,通过配置客体属性区分独占式客体和共享式客体来解决资源访问冲突问题,客体访问控制参考类图如图5所示。

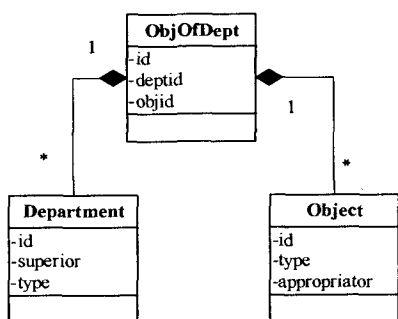


图5 客体访问控制参考类图

3 MO-RBAC模型应用

相对于传统的RBAC模型,MO-RBAC模型更适于应用在矩阵型组织环境内。下面以某科研项目管理信息系统为例,简要介绍MO-RBAC模型的应用。

该科研项目管理信息系统开发对象是某科研单位,该单位采用如图1所示的强矩阵型管理模式来管理各科研项目的开发工作。其具体工作流程为:

(1)每个科研项目都指定了一个专职的项目主管,全权负责该项目整个生命周期的执行和监督工作。

(2)项目主管直接向各部门主管下达工作任务,并监督这些任务的执行。

(3)各部门主管再根据这些分配给本部门的工作任务向各下属各科室主管下达工作任务。

(4)各科室主管最后根据分配给本科室的任务为各工作人员分配工作并进行监督管理和资源调配工

作,最后由科室主管负责统计工作中的消耗和花费并将执行情况和结果上报给上级职能部门。

(5)各职能部门要向项目主管反馈分配的任务在本部门的运行状况和花费。

从上述工作流程可以看出,该系统用户角色繁多,相关权限管理和操作限制复杂,对数据的安全访问限制也比较多。为此在该系统中应用了MO-RBAC模型,定义了项目主管、部门主管、科室主管等多种角色并为每个角色定义了操作约束,用户根据登录系统时所赋予的角色和部门来执行相关操作,并根据角色和部门的偏序关系及访问控制约束机制来查询和使用任务数据和其它资源。

另外,采用角色和部门的共同约束机制也很好地解决了项目管理人员组合随意性比较大等问题,使得系统具有很好的适应性。该系统已交付运行3年左右,使用效果良好。

4 结束语

分析了传统的RBAC96模型在矩阵型管理组织模式中的一些不足之处,提出了一种改进的访问控制策略,该模型对RBAC模型进行了扩展,通过部门——角色约束机制以及部门——客体映射机制,较好地解决了在矩阵型组织模式下的进行权限建模和系统伸缩性等问题,使模型能够更好地适应企业运行的需要。

参考文献:

- [1] 张翼飞. 基于矩阵型组织的项目管理信息系统的研究与实现[D]. 沈阳: 沈阳航空工业学院计算机学院, 2005.
- [2] Ferraiolo D, Kuhn R. Role-Based Access Control[M]. London: Artech House, 2003.
- [3] Sandhu R. Role-Based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47.
- [4] 徐震, 冯登国. 一种使用组织结构的访问控制方法[J]. 计算机工程, 2006, 32(13): 20-22.
- [5] 陈刚, 陈长琴. 基于角色和部门的两级访问控制模型[J]. 武汉科技大学学报: 自然科学版, 2006, 29(4): 398-400.
- [6] 唐柳英, 卿斯汉. 混合RBAC-DTE策略的多角色管理[J]. 软件学报, 2006, 29(8): 1419-1426.

(上接第179页)

- [5] 唐国坪, 廖晓峰. 基于混沌映射的抗剪切鲁棒水印算法[J]. 计算机工程, 2005, 31(9): 34-36.
- [6] 李传目, 洪联系, 万春. 基于混沌序列的图像分块加密方法[J]. 计算机技术与发展, 2007, 17(8): 51-54.

- [7] 刘树田, 孙凯霞, 任宏武. 分数傅立叶变换的数值模拟算法[J]. 计算物理, 1997, 14(6): 760-764.
- [8] May R M. Simple mathematical model with very complicated dynamics[J]. Nature, 1976, 261: 459-481.