# 基于 FTP 的图像混沌加密传输技术的实现

刘新杰，李黎明
（广东工业大学，广东 广州 510006）

**摘 要**：为了提高混沌图像加密传输系统的传输速度并扩大应用范围，提出了一种实现混沌图像加密传输的新方法：利用 VSFTPD 软件在 Mini 2440 ARM 平台上构建 FTP 服务器，通过 FTP 实现混沌加密图像数据的传输。实验结果表明，该系统能够实现混沌加密图像的可靠快速传输。

**关键词**：文件传输协议；ARM；混沌加密；图像
**中图分类号**：TP302 **文献标识码**：A **文章编号**：1674-7720(2014)04-0047-03

## Implementation of transmitting chaotic-encrypted image based on FTP

Liu Xinjie, Li Liming
(Guangdong University of Technology, Guangzhou 510006, China)

**Abstract**: In order to accelerate the rate of chaotic-encrypted image transmission system and extend its field of application, this paper proposes a new method of transmitting chaotic-encrypted image: applying VSFTPD software to Mini 2440 ARM platform to setup a FTP server, and using FTP to convey the encrypted image files. The experiment result shows that this system can transfer chaotic-encrypted images rapidly and reliably.

**Key words**: file transfer protocol; ARM; chaotic encryption; image

计算机和网络技术的飞速发展使得上网设备的体积越来越小，手机购物、手机支付在生活中的应用越来越广泛。智能手机、平板电脑运行的是嵌入式操作系统，因此嵌入式设备在移动网络中的信息安全逐渐受到人们的关注。个人的隐私信息一旦被窃取，将会造成很大的损失。而当前比较成熟的 DES、AES 等加密算法主要针对 PC 平台设计，不适合直接应用于嵌入式设备中。

混沌系统具有对初始条件高度敏感性和遍历性的特点，可以实现同步控制，因此非常适合进行数据的加密传输[1]。当前，国内外对于嵌入式平台上混沌加密技术的应用研究非常广泛，关于混沌加密技术的研究已经比较成熟。但是当前多数加密系统是通过简单调用 Socket API 函数编程实现网络传输的，其速度较慢且不适合在广域网中使用。而混沌系统对初始值敏感的特性，使得快速网络传输具有一定的不可靠性。因此，设计一个既能够实现混沌加密，又能够进行快速可靠网络传输的通用混沌保密传输系统是非常有必要的。FTP 是 TCP/IP 的一种具体应用，工作在应用层，是基于 TCP 的服务，使用的是 Client/Server 工作模式，可以在不同平台之间提供可靠的网络传输服务。FTP 在网络中的应用已经非常成熟，因此可以和混沌加密技术结合起来实现网络内混沌加密数据的可靠传输。

## 1 硬件实验平台

硬件平台使用的是友善之臂公司的 Mini 2440 开发板，集成了基于 ARM920T 架构的 Samsung S3C2440A 处理器，64 MB 的 SDRAM、2 MB Nor Flash 和 256 MB Nand Flash，配置了 LCD 显示器，并集成了 DM 9000 网络芯片，用于支持网络传输。RS232 串口用于交叉开发过程中计算机与开发板之间的通信。该系统使用两块 Mini 2440 开发板，其中一块配置为 FTP 服务器，另一块配置为客户端。服务器与客户端通过路由器实现网络传输。硬件系统框图如图 1 所示。

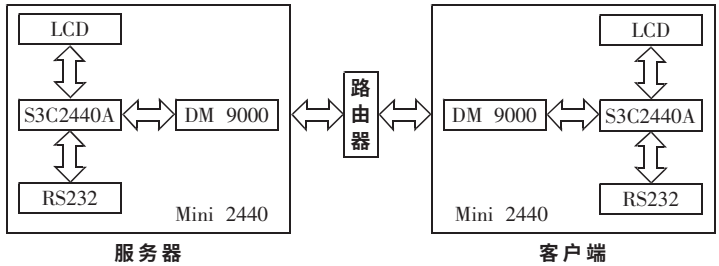


图 1 硬件系统框图

## 2 混沌图像加密原理

混沌图像加密的原理如下：利用混沌系统的差分方程进行迭代运算，期间产生的变量序列用于生成加密密钥，与要加密的图像数据进行相应的运算实现数据的加密。在接收端进行相应的逆运算即可解密得到原始图像。产生的加密密钥又称为混沌序列，因此该方法称为混沌序列加密。由于混沌系统具有遍历性和非周期性，生成的加密密钥具有伪随机特性。

数字图像的加密方法主要有两种：第一种是直接加密算法，即将图像看作普通的数据直接进行加密，不利用图像数据的任何特性，对所有的数据进行加密处理；第二种是选择性加密算法，即在加密过程中，有选择性地加密图像的一部分关键数据。直接加密算法具有很高的安全性，加密之后数据格式被破坏，窃听者无法获知传输的数据格式，其缺点是加密速度较慢。选择性加密算法则保持了原有的数据格式信息和控制信息，只加密实际数据部分，因此具有良好的相容性。本系统使用的是选择性加密算法。

混沌序列是由混沌差分方程迭代产生的，因此混沌系统的设计非常重要。参考文献[2-3]提出了基于改进的 Wang-Chen 算法的离散混沌系统产生混沌序列的方法。服务器端使用的混沌系统方程如下：

$$\begin{cases} \dot{x}^{(1)}=0.2x^{(1)}-0.3p+0.1z^{(1)}+e\times\sin(dp) \\ \dot{y}^{(1)}=0.3x^{(1)}-0.2y^{(1)}-0.1z^{(1)} \\ \dot{z}^{(1)}=-0.1x^{(1)}-0.1p+0.2z^{(1)} \end{cases} \tag{1}$$

其中 $e=1.0\times10^5$、$d=20.0$ 是混沌系统的参数。该系统使用的是驱动-响应式同步方法，服务器端方程中的 $y^{(1)}$ 变量经过多次迭代产生一系列的数值，经过处理后生成混沌加密密钥，与图像数据进行加法运算后得到 $p$，即加密后的图像数据。将加密后的图像利用 FTP 传输到客户端后，利用接收到的加密数据 $p$ 驱动接收端的混沌系统，使两端的系统同步。最后用加密数据 $p$ 与客户端 $y^{(2)}$ 变量生成的混沌序列进行相应的逆运算，即可解密得到原始的图像数据。客户端使用的混沌系统方程如下所示：

$$\begin{cases} \dot{x}^{(2)}=0.2x^{(2)}-0.3p+0.1z^{(2)}+e\times\sin(dp) \\ \dot{y}^{(2)}=0.3x^{(2)}-0.2y^{(2)}-0.1z^{(2)} \\ \dot{z}^{(2)}=-0.1x^{(2)}-0.1p+0.2z^{(2)} \end{cases} \tag{2}$$

## 3 FTP 服务器的构建

VSFTPD(Very Secure FTP Daemon)是一种开放源代码的 FTP 服务器，广泛地应用于多种 UNIX 和 Linux 操作系统[4]。与其他开源的 FTP 服务器相比，VSFTPD 可以提供更加安全易用的文件传输服务，因此在 Linux 系统中得到了广泛的使用。

在官方网站下载源代码文件后，需要经过编译将其移植到 Mini 2440 开发板上。首先修改 Makefile 文件，将 CC 字段更改为交叉编译工具 arm-linux-gcc；然后需要修改 vsf_findlibs.sh 文件，并且将用到的动态库从编译器文件夹下复制到要制作的根文件系统中；生成 vsftpd 文件后，配置 vsftpd.conf 文件。需要注意的配置选项有几个，其中，anonymous_enable 选项配置为 YES，即允许匿名用户登录 FTP 服务器；local_enable 选项配置为 YES，即允许本地用户登录；write_enable 选项设置为 YES，即允许各种 FTP 写入命令；listen 选项设置为 YES，即设置 FTP 服务器工作在 standalone 模式，进程自动监听 FTP 请求[5]。

完成以上步骤后，将 vsftpd 和 vsftpd.conf 分别复制到根文件系统的/sbin 和/etc 目录下。最后利用 busybox 制作根文件系统[6]。如图 2 所示在配置过程中要选择 busybox 对 ftpput/ftpget 命令的支持，用于客户端与服务器之间文件的传送。

图 2 busybox 配置选项

由于在配置内核时将 DM9000 芯片的 MAC 地址、IP 地址等设置为固定值，如果不做修改，两块开发板会发生地址冲突。可以在根文件系统的 rcS 文件中利用 ifconfig 命令将两块开发板的地址设置为不同的值：客户端的 MAC 地址设置为 00:11:22:33:44:55，IP 地址为 192.168.1.230；服务器端的 MAC 地址为 08:90:90:90:90:90，IP 地址为 192.168.1.235。图 3 所示为客户端开发板对应的文件设置。

```
ifconfig lo 127.0.0.1
ifconfig eth0 hw ether 00:11:22:33:44:55
ifconfig eth0 192.168.1.230 netmask 255.255.255.0 up

route add default gw 192.168.1.1
/bin/hostname -F /etc/sysconfig/HOSTNAME
"etc/init.d/rcS" 20L, 438C
```

图 3 客户端 MAC 和 IP 地址的设置

将编写的混沌加密程序文件复制到服务器端的根文件系统中，将解密程序复制到客户端的根文件系统中。利用友善之臂提供的 mkyaffs2image 工具分别制作根文件系统并烧写到对应的开发板上。

将根文件系统烧写至开发板后，还要在服务器端进行设置。VSFTPD 服务器要求服务器端有 nobody 和 ftp 两个用户，而且需要在/usr/share 目录下创建 empty 目录，在/var/log 目录下创建 vsftpd.log 日志文件。

## 4 混沌保密传输系统的验证

将两块开发板通过路由器连接成为一个简单的局域网。服务器端对图像文件进行加密后，将加密后的数

据放在 FTP 目录下面，然后运行“vsftpd &”指令，开启 FTP 服务器并使进程在后台运行。客户端使用 ftpget 命令从服务器端获取加密后的图像数据，并运行解密程序得到解密后的图像。实际硬件连接图以及加密效果如图 4、图 5、图 6 所示。

图 4 加密传输系统实际效果图（左为服务器，右为客户端）


图 5 服务器端的原始图像和加密后的图像

服务器端的原始图像为经典的 Lena 图像，在客户端通过 FTP 获取加密后的图像后，利用解密程序可以很好地还原出原始图像。

该系统的特点是利用 FTP 服务实现局域网内的混沌保密通信。经过验证，该系统能够利用 FTP 服务将混沌加密的图像数据可靠地传输到接收端。由于 FTP 在广域网中的应用已经非常成熟，因此该系统比较容易扩展至广域网中，进一步推动了混沌加密系统的实用化，具有很好的应用前景。


图 6 客户端接收到的加密图像和解密后的图像

参考文献

[1] 王光义，袁方.级联混沌及其动力学特性研究[J].物理学报，2013，62(2)：111-120.

[2] 陈关荣，汪小帆.动力系统的混沌化——理论、方法与应用[M].上海：上海交通大学出版社，2006.

[3] 凌大旺.基于离散混沌映射的数字图像加密技术研究与实现[D].广州：广东工业大学，2012.

[4] 杨明华.Linux 系统与网络服务管理技术大全[M].北京：电子工业出版社，2010.

[5] 罗彩君.基于 Linux 系统的 FTP 服务器的实现[J].电子设计工程，2013，21(11)：40-41.

[6] 韦东山.嵌入式 Linux 应用开发完全手册[M].北京：人民邮电出版社，2008.

（收稿日期：2013-10-28）

作者简介：

刘新杰，男，1990 年生，在读硕士研究生，主要研究方向：混沌图像保密通信。

李黎明，男，1985 年生，在读硕士研究生，主要研究方向：混沌视频保密通信。