一种新型非线性视频图像交叉加密算法*)

徐建波[1,2] 梁 伟[1] 朱理望[1] 向德生[1]

(湖南科技大学计算机科学与工程学院 湘潭 411201)[1] (湖南大学计算机与通信学院 长沙 410082)[2]

摘 要 为了改善视频图像加密的安全和实时性能,提出了一种基于非线性的视频图像交叉加密算法。针对混沌系统中存在有限精度效应的影响和线性反馈移位寄存器生成序列的线性复杂度非常有限并且容易破解的问题,结合混沌技术和线性反馈移位寄存器技术,构造了非线性交叉加密算法的理论数学模型,阐述了算法的设计原理,介绍了实现的相关代码。通过与其他传统算法的理论分析和硬件实现的性能比较,结果表明:产生的视频图像密码序列在较低迭代次数来得到周期极大的非线性序列密码,其总体性能比可达到 0.68,因此为高性能视频图像的传输提供了一种新的安全实时加密方法。

关键词 交叉加密算法,混沌技术,线性反馈移位寄存器,序列密码

New Type of Non-linear Video Images Cross-encryption Method

XU Jian-bo[1,2] LIANG Wei[1] ZHU Li-Wang[1] XIANG De-sheng[1]

(School of Computer Science and Engernering, Hunan University of Science and Technology, Xiangtan 411201,China)[1]

(School of Computer and Communication , Hunan University,Changsha 410082,China)[2]

Abstract For improving security and the real time function of encrypted video image, brings forward one kind of the non-linear crossing encryption algorithm. In allusion to the limited accuracy effect in chaotic system and the very limited linear complexity degree of generating sequence of linear feedback shift register, which is decoded easily, integrate chaos system and linear feedback shift register technology , construct a non-linear cross-encryption algorithm theory mathematic model, expound algorithm design principle, present the relevant implement code. Comparing with traditional algorithms by theoretical analysis and hardware implement result, video image cipher brought by this type of encryption algorithm is a non-linear sequence which presents a very long cycle after a few iteration implement turns , the overall performance ratio can point to 0.68,so a new type of secure rapid encryption method applied to transport of high-performance video image has come into being.

Keywords Cross-encryption algorithm,Chaos technology,Linear feedback shift register,Stream cipher

1 引言

随着基于嵌入式设备的视频流[1,2]迅猛发展,加密算法一直在信息安全领域起着非常重要的作用。目前,国内外信息加密普遍采用基于密钥的算法,如 RSA,AES 算法等,但它们存在着一定的缺陷。尤其对于视频图像、语音等多媒体这样的大容量信息而言,原有的传统数据加密算法[3-6]在实现速度、安全性能、资源使用量和跨平台性等方面均难以继续满足新的应用需求。

近年来,人们将研究的目光转向了混沌系统和线性反馈移位寄存器加密算法。混沌系统中将混沌映射用于加密有着非常优越的性能。混沌有着对初始条件和参数敏感、伪随机性和遍历特性等特点,利用它来设计序列密码或分组密码,特别是利用混沌的拓扑传递性来快速地置乱和扩散明文数据,以达到随机改变明文统计特性的目的。而线性反馈移位寄存器由于 m 序列的长周期和良好的随机统计特性,因此在序列密码中应用广泛。虽然混沌映射算法[7,8]在混沌序列产生的理论研究已经很成熟,但是混沌序列发生器总是在有限精度下实现,混沌迭代过程过多,必将变换为较小的周期序列。因此,要想进一步获得更大周期的混合混沌序列,一方面可用较低混沌迭代次数来实现精度系统,另一方面也可通过增大 LFSR 的级数来增大周期,使其周期随 LFSR 的级数增大而呈指数递增,最终输出较大的非线性序列周期。

2 改进交叉加密算法的设计

2.1 算法的数学模型

定理 1 LFSR 的周期只与其反馈方式有关,而不依赖于其初始状态[7]。

根据其反馈方式的不同,可以定义 LFSR 的特征多项式:

$$P(x)=\sum_{i=0}^{m} f_i x_i = x_m + f_{m-1}x^{m-1} + \cdots + f_i x + 1 \qquad (1)$$

其中 $f_n=f_0=1, m=0,1,2,3\cdots$

定理 2 混沌系统中 Logistic 映射可以用一维非线性函数来表示其混沌行为,通过微小的参数调节来产生完全不同的随机序列,函数可表示为

$$x_{n+1}=\lambda x_n(1-x_n) \qquad (2)$$

*)国家自然科学基金项目(60673061),湖南省自然科学基金项目(02JJY5006),湖南省教育厅科学研究项目(07C271)资助。**徐建波** 教授,主要研究方向为计算机网络、信息安全与嵌入式系统;**梁 伟** 硕士,讲师,主要研究方向为信息安全和嵌入式系统;**朱理望** 高级工程师,主要研究方向为图像处理与 EDA 工程设计;**向德生** 副教授,主要研究方向为计算机视觉和图像处理。

其中 λ 为调节参数，$\lambda\in(0,4)$，$x_n\in(0,1)$ $n=0,1,2,3\cdots$

从(1)式可以看出 LFSR 的级数，一般高精度的实现系统必然以高成本为代价，而(2)式中混沌函数的短周期，为获得相同的周期，有限精度的混沌函数内部要比移位寄存器使用多一倍的存贮器数目。那么如何在视频图像加密的基础上既能使系统具有更高的安全特性，又能保持较高的执行速度呢？为此，我们在文献[7,8]的基础上提出了改进算法，新算法公式为

$$f(x,\lambda,\alpha,\beta)=\lambda\times\mathrm{tg}(\alpha x)\times(1-x)^{\beta} \tag{3}$$

可以通过实数值序列方法来确定序列，即$\{x_k,k=0,1,2,3\cdots\}$是混沌映射的轨迹点所形成的序列。令 $m=n+1$，则有

$$P(X)=\sum_{i=0}^{n}f_i=\lambda x_{n+1}(1+x_{n+1})+f_n x^n+f_n x^n+L+f_i x+1 \tag{4}$$

$$f(x,\mu,\alpha,\beta)=\mu\times\mathrm{tg}(\alpha x)\times(1-x)^{\beta} \tag{5}$$

2.2 新型视频图像加密算法的分析

通过传统的视频图像加密方法的分析和比较，我们可以提出一种新型图像加密方法，其产生方法结构原理图如图 1 所示。该方法是混沌序列发生器和 LFSR 序列发生器以异或方式的结合。LFSR 序列具有良好的随机性，而混沌序列发生器由 Logistic 映射算法实现。两种发生器以简单的数字逻辑操作进行交叉运算。

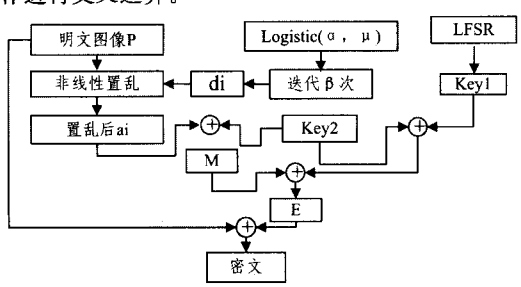


图 1 视频图像加密算法加密原理结构图

在加密过程中，密钥的生成过程为：用户输入的密码用 LFSR 算法加密，选取高度线性不相关的多项式左移产生一系列数据作为密钥。假设用户密码为 s(为了提高安全性，长度最好大于 8 个字节)，线性移位寄存器中每个字节的多项表达式为

$$y=x+x^2+x^5+x^7 \tag{6}$$

所有字节的多项表达式为

$$z=1+y^3+y^5+y^7 \tag{7}$$

整个数组向左移一位，我们就可以得到一个字节的数据，依次类推。经过多次线性左移循环，我们就可以得到一系列数据，记为 Key1 和 Key2，作为初始密钥。

为了提高安全性，通过视频图像关键帧时间戳的变化而产生的动态密钥来进行加密数据。一般我们取出关键帧 I 的时间戳与 256 的余数作为 LFSR 序列发生器中左移或右移的次数，这样得到的动态加密密钥就完全不同。接着需要加密的数据与产生的密钥一一异或加密，然后根据混沌序列发生器中的连续实数集上的非线性变换来提高序列密码的随机性和密钥长度。定义的相关表达式如下：

$$Count=I_{\mathrm{time}}\%256 \tag{8}$$

$$Key1=LFSR(count) \tag{9}$$

$$data=key\wedge data \tag{10}$$

(8)式中的 I_{time} 表示 I 帧的时间戳，(9)式中的 $LFSR$ 表示线性移位寄存器左移或右移，$count$ 次产生的密钥，(10)式中的 $data$ 表示需要加密的 I 帧数据。

在有初始密钥和控制信号的作用下，输入待加密的图像数据块，加密前的信息可作为明文图像信息，如图 1 所示，整个加密系统主要由原始明文信息、LFSR 序列发生器(10 位)、混沌序列发生器(10 位)组成。加密过程为：从原始明文信息和 LFSR 序列发生器 A 中取出一个序列作为密钥 Key1，再从混沌序列发生器 B 中取出一个序列作为密钥 Key2，两者做异或运算，用新生成的序列作为总密钥 Key=Key1+Key2。接着对第 2 个序列做类似运算，直到存储 P 中的有效图片信息全部运算完毕为止。至此，信息 P 已被 LFSR 序列和混沌序列进行初步加密，生成的密钥 Key2 进行第二次异或运算，并形成了中间结果 M，然后利用总密钥 Key 和类似的异或算法对 E 进行最后加密，形成密文。解密过程是加密过程的逆运算，在此不再描述。部分核心代码描述如下：

```
void encyption (struct param_table, char ID[]) //param_table 参数表,ID 用户密码
{
 select_param(param_table); //选择参数
    key= init_key(ID); //用户输入密码初始化
   while(有加密数据时)
    {
     LFSR(key1);//移位寄存器移位生成密钥
    Logistic(key2);//混沌序列发生器生成密钥
     Key=key1^key2;
        Sbox(key); //非线性变换
key_data = encryption(data,key);//明文与密钥加密
        Output(key_data); //输出密文
    }
}
```

3 仿真时序分析及图像实验结果比较

对于新型视频图像加密算法的实现是在实际的 FPGA 硬件系统上运行的。该算法采用硬件描述语言进行设计，用 VHDL 语言编写其相关程序，然后在 quartus5.1 平台上完成了调试编译和模拟工作。在对图片加密的功能测试中，我们得出了如图 2 和图 3 的时序仿真图。

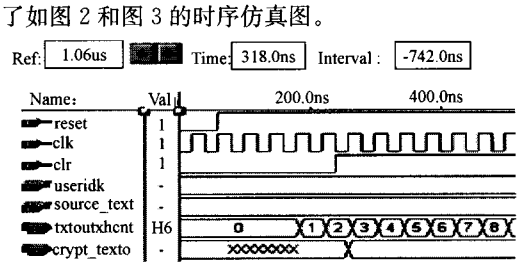


图 2 初始化阶段时序图

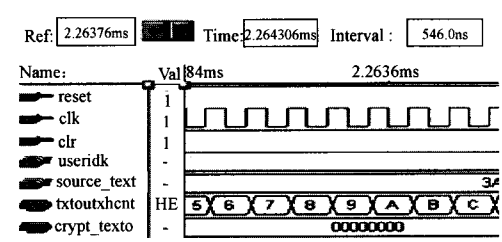
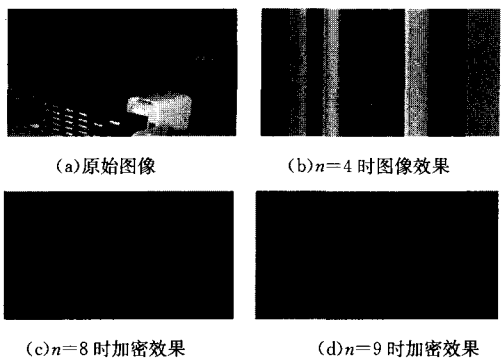


图 3 128 位明文加密时序图

图 2 中列出了图像信息在本文算法的基础上加密的时钟信号、1k、初始密钥 USEidk 以及 128 位明文输入信号 source_

text、密文输出信号 crypt_texto，其中密文分 4 次输出，每次输出 128 位，扩散操作后的数据在图中以蓝白显示。从图 3 中可以看出，图像加密数据以不同的时钟间隔输出，例如产生第一批 128 位密文数据输出消耗 56575 个时钟周期，耗时 2.263ms，这一点与传统序列密码的数据输出方式不同。这主要是通过增大 LFSR 的级数使周期增大，同时在非线性置乱模块中，应用混沌迭代获取敏感数值的精度过程中引入了周期时间延时而导致的。

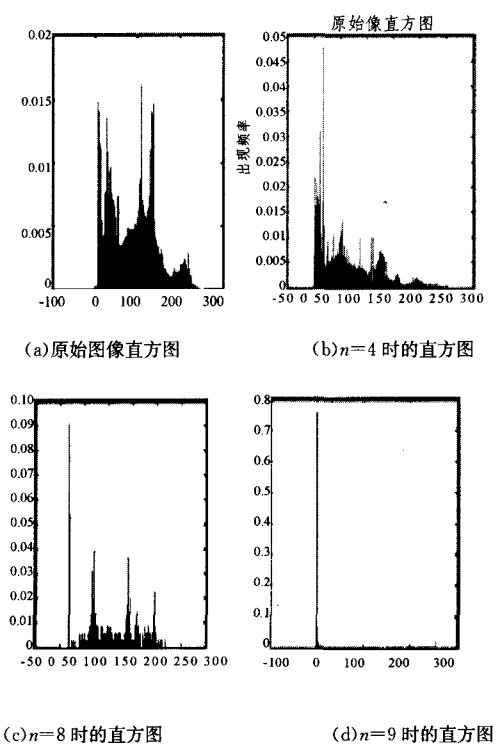


(a)原始图像　(b)n=4 时图像效果

(c)n=8 时加密效果　(d)n=9 时加密效果

图 4　图像加密效果图

以一幅大小为 64×64 的 256 色的一帧视频图片为例进行算法的加密效果演示。从图 4 可以看出，每一帧图片经过 n 轮循环加密。来实现视频图像加密，随着轮数的增加，改变幅度减小，但加密性能继续增强。但是这种性能的增强变化并不是无限制的。在本文设计方案中，加密轮数设为 9 时，图像加密的综合性能最佳。而从图 5 中 n 取不同值时也可以从其直方图看出，当 n 的值超过 8 时，直方图中波形的大小变得较为平缓和均匀，因此在视频图像加密设计中交叉加密算法应根据实际的需求来合理选择加密轮数，以获得最优的性能比。



(a)原始图像直方图　(b)n=4 时的直方图

(c)n=8 时的直方图　(d)n=9 时的直方图

图 5　图像加密灰度直方图

为测试算法的性能，采用 Visual C++语言，在配置为 Pentium IV2.4GHz，512 MB RAM 的 PC 机上实现，Logistic 混沌映射中取 u=4，我们用两个不同类型、不同大小的文件进行加密，然后解密实验，记录下有关的数据，并与另外两个相似的混沌加密算法(文献[9]和文献[10]中算法)进行比较。所用到的文件是：一帧视频图像文件，大小为 128kB。

表 1　算法对图像文件加密后的性能比较

算法加密时间(s)	文献[9]	文献[10]	本文
移位/迭代次数	36875	7409	3461
密文非线性置乱程度	302	298	579
密文大小(kB)	296	264	256

针对图像文件运用三种算法的加密结果见表 1。从表中可以看出，本文所提算法最快，其次是文献[9]中的算法，而文献[10]中的算法运行速度太慢，不适合加密现在广泛使用的视频图像文件，更不适合在 Internet 网上运行。而且本文所提算法在密文的大小、密文的非线性置乱程度和密文移位/迭代速度方面都明显优于前面两种算法。

结束语　针对嵌入式设备和视频流的特点，在保证流畅的视觉效果的同时，视频图像加密算法不仅需要考虑实时在线能力，而且要求具有很高的处理速度。本文设计并实现了一种新型视频图像交叉加密算法。通过实验数据仿真和性能评估比较，此快速算法具有如下的优点：①快速有效地加密；②在嵌入式设备中占用资源很少，加密过程中能保持较低迭代次数；③该算法的提出和实现，大大改善了嵌入式应用设备中视频图像安全性问题和实时性要求，因此该算法能够应用于广泛的视频图像加密领域。

参 考 文 献

[1] Carlos J, Pimentel L, Monroy R, et al. A Method for Patching Interleaving-Replay Attacks in Faulty Security Protocols[J]. Electronic Notes in Theoretical Computer Science, 2007, 174(4): 117-130

[2] Huang K H, Chien S C, Hsu Y N, et al. A Total Laboratory Automation System Consolidated by Virtual Private Network for Improving Laboratory Efficiency[J]. WSEAS Transactions on Systems, 2007, 6(2): 310-315

[3] Jakimoskig, Kocare V L. Chaos and cryptography: Block Encryption Ciphers Based on chaotic Maps. Circuits and Systems I: Fundamental Theory and Applications[J]. IEEE Transactions on, 2001, 48(2): 163-169

[4] 陈刚，赵晓宇，李均利. 一种自适应的图像加密算法[J]. 软件学报，2005，16(11)：1203-1208

[5] HUANG Guang-hua, NI Guo-qiang. A Realistic Image Rendition Method Based on the Cone Adaptation Model[J]. Journal of Image and Graphics, 2007, 12(7): 1160-1167

[6] 黄光华，倪国强. 一种基于视频适应模型的真实影像再现方法[J]. 计算机图象图形学报，2007，12(7)：1160-1167

[7] 高江，张宜生，梁书云，等. 一种新的混沌加密算法及其应用[J]. 小型微型计算机系统，2006，27(4)：655-657

[8] Sempere V, Albero T, Silvestre J. Analysis of communication alternatives in a heterogeneous network for a supervision and control system. Computer Communications, 2006, 29(8): 1133-1145

[9] Alvarez E, et al. New approach to chaotic encryption. Phys. Lett, 1999, A263(4/6): 373-375

[10] Liu Jun, Mou Xuanqin, Cai Yuanlong. Improving ecurity of a chaotic encryption approach. phys. lett, 2001, A 290(3/4): 127-133