文章编号:1000-582X(2008)10-1189-05

用混沌映射的图像加密算法实现 FPGA

廖晓峰,岳　蓓,周　庆,南　海
(重庆大学 计算机学院,重庆 400030)

摘　要:为了解决数据信息量大的多媒体加密系统软件不能满足实时性要求这一问题,提出了一种适宜于硬件加密的基于 Kolmogorov 混沌映射的图像加密算法——MASK(mix add Sbox kolmogorov),并将整个算法在 Cyclone EP1C6 FPGA(field programmable gate array)上实现。该算法由 4 个基本变换组成,M 变换、A 变换、S 盒变换和 K 映射变换,分别具有扩散、加密钥、非线性和置乱的效果。随后就整个算法安全性在相邻象素的相关性、UACI 和密钥空间等方面进行了讨论,并统计得到算法的硬件实现的资源占用率较低。实验结果说明该系统具有安全性高、加密速度快、硬件资源消耗小等优点,适用于低端 FPGA 硬件的开发。

关键词:密码学;混沌理论;图像处理;FPGA
中图分类号:TP 309.7　　文献标志码:A

An field programmable gate array implementation of an image encryption algorithm based on a discrete chaotic map

LIAO Xiao-feng, *YUE Bei*, *ZHOU Qing*, *NAN Hai*
(College of Computer Science, Chongqing University, Chongqing 400030, P. R. China)

Abstract: Software encryption cannot satisfy real-time requirements for multimedia applications which usually involve large volumes of data. To address this problem, an field programmable gate array(FPGA) implementation of the Cyclone EP1C6 for a Kolmogorov chaotic map-based image encryption algorithm MASK was proposed. The algorithm was composed of four basic parts: Mixture, key Add, S-box and Kolmogorov chaotic map transforms. These parts specifically act on the image as follows: diffusion, applying secret keys, nonlinearity, and permutation. The correlation of adjacent pixels, UACI and the key space of the system subsequently were studied. The source occupation proportion of the hardware was calculated statistically and showed low occupation. Among the advantages of the proposed system are high security, fast encryption speed, and low hardware resources consumption. The proposed system is suitable for implementation in inexpensive FPGA.

Key words: cryptography; chaos theory; image processing; field programmable gate array

随着科技的进步与 Internet 的普及,数字图像已经越来越普遍地应用于人们日常生活中。由于数字图像能够很容易地进行复制、篡改和大量传播,对数字图像的保护也日趋成为一个重要的问题,而图像加密技术则是解决该问题重要手段之一。

图像加密最直接的方法是使用传统的分组加密

收稿日期:2008-05-25
基金项目:国家自然科学基金资助项目(60573047);重庆市自然科学基金资助项目(8509);重庆大学研究生创新基金资助项目(200609Y1B0150174)
作者简介:廖晓峰(1963-),男,重庆大学教授,主要从事计算机图像处理等方向研究,(Tel)13752937210;
(E-mail) opalus413@126.com

算法(如DES或AES算法)[1-2]对图像进行加密。但这种方法没有充分考虑图像本身的特点,仍有2个缺点需要克服。一是分组加密算法相当于对固定长度分组的替换运算。对于图像这种冗余性大的数据,加密后由于具有很强的"块"效应,在许多情况下仍然可以从加密后的图像中看出原始图像的轮廓。二是分组加密算法要进行多轮加密,而每一轮加密又没有利用图像的空间特性,使得图像的加密速度较慢。

由于混沌系统特有的随机性、初值敏感性和各态历经性,再加上非常简单,被广泛应用于图像加密技术[3-10]。例如Pichler和Scharinger提出了一种在扩散操作前的基于Kolmogorov映射的图像置乱算法[3-4];Chen等人提出了基于3D cat映射的图像加密算法[9];Lian提出了基于standard映射的算法[1]。这些算法充分利用了图像的空间特性,大大提高了图像加密的速度。另一方面,由于混沌系统具有很强的初值敏感性,也使得图像微小的变化也可很快地扩散到整个图像。但混沌映射通常需要大量的乘除运算,这些操作会降低加密算法的速度。再加上面对图像视频之类具有庞大的数据量的原始处理数据,软件的实现已不能满足实时性的要求,用硬件实现已成为实时图像加密更好的选择[11-13]。

图像加密算法的硬件实现至少有两种备选方案,即专用集成电路(application specific integrated circuit,ASIC)和现场可编程门阵列(field programmable gate array,FPGA)。FPGA相对ASIC的优点在于快速的开发周期、低成本的开发投资和可重复编程[14-16]。针对此图像加密系统的特点和成本投资,选择FPGA作为硬件实现,通过FPGA来实现编程灵活性、物理安全性和比软件更高的速度等要求。

1 离散混沌映射加密算法及其分析

图像加密算法由预备变换、多轮加密和最后一轮构成。预备变换即对整个图像进行K变换。在多轮加密的每一轮中,将图像分成若干处理单元(PE),对每个PE分别进行M、A和S变换;最后对整个图像进行K变换。最后一轮对图像进行M、A、K变换。以上涉及的4个变换M、A、S和K具体操作如下:

1.1 混合M变换

将PE中的每个元素加起来,即:

$$\mathrm{Sum(PE)}=\sum_i\sum_j pe_{ij}\ 。\tag{1}$$

然后将Sum(PE)与每个元素进行加操作后的结果覆盖此元素,即:

$$pe_{ij}=\mathrm{Sum(PE)}+pe_{ij}\ ,\tag{2}$$

此变换可以达到一个元素pe_{ij}的变化影响到整个处理单元PE的目的。

1.2 加A变换

生成与PE大小相同的密钥K,让K与PE进行加操作,即:

$$C=\mathrm{PE}+\mathrm{K}\ 。\tag{3}$$

注意式(1)~(3)中定义的"+"操作是有限域上的广义加法运算。此加变换达到通过密钥保护图像的目的。

1.3 S盒置换

以PE中每个元素的值做为S盒的地址,取出此地址的值来替换原元素,即

$$pe_{ij}=\mathrm{Sbox}(pe_{ij})\ 。\tag{4}$$

此变换是4个操作中惟一一个非线性变换,有很好的扩散和混乱性能[10]。

1.4 K变换

Kolmogorov变换,又被称为generalized Baker映射,原理是将PE中位于坐标$(x,\ y)$的元素置乱到PE中的另一位置$T_{\mathrm{no}}(x,y)$,即

$$T_{\mathrm{no}}(x,y)=(p_{\mathrm{s}}(x-F_{\mathrm{s}})+(y\bmod p_{\mathrm{s}}),\ F_{\mathrm{s}}+(y\ \mathrm{div}\ p_{\mathrm{s}}))\ 。\tag{5}$$

其中,$O=(n_1,n_2,\cdots n_k)$,即将图像划分成多个以n_i为宽度的单元块;$P_{\mathrm{s}}=N/n_{\mathrm{s}}$,$N$为图像的边长;$F_{\mathrm{s}}=\mathrm{n_1}+n_2+\cdots+n_{\mathrm{s}}$,当$s=0$时,$F_0=0$。

1.5 算法分析

在以上的4个变换中,M、A和S变换可以有效地实现对每个PE内的扩散和混乱的要求,而K变换进一步将这每个PE内的扩散和混乱扩大到整个图像中,提高图像加密的安全性。

在4个变换中M和A变换只涉及有限域上的加法运算,在实现中可选用异或等快速指令来实现。S变换是简单的替换操作,速度很快。K变换虽然使用了除法和模运算,但在实现中也可转换为替换操作。

另一方面,图像解密过程与加密过程在结构上是完全相反的,但都是由4个基本变换操作组成,所以只需要控制这些基本操作的顺序即可,这可大大减少硬件所需的资源(等价于逻辑门数),从而降低硬件实现的成本。因此该算法在安全性、速度和成本上都非常适合于在FPGA上实现。

2 图像加密算法的硬件设计

2.1 系统的总体设计

一个图像加密系统一般需要3个部分,输入单

元，输出单元，加密单元和控制单元。针对所使用的硬件设备，输入单元由一个 RAM 模块提供，将所需要进行加密的图像存储于此模块内，并以此作为中间数据的存储空间。输出单元则控制 LCD 的显示，将加密前后的图像显示于液晶显示屏上。加密单元包括对加密算法的设计。加密算法需要 4 个基本的变换操作，即 MASK 变换，在设计中需要分别对这 4 个部分设计单独的处理模块，而对这 4 个部分的顺序控制及数据通讯的处理则由控制单元的控制模块来完成。

控制模块是整个系统的控制总线，分别通过五条主控制线启动 M、A、S、K 和 LCD 模块的使能信号，并输入是否解密操作信号，使得各模块从 RAM 中读取原数据，在各操作模块中根据不同的功能处理原数据，最后再将结果存入 RAM 中，如图 1 所示。

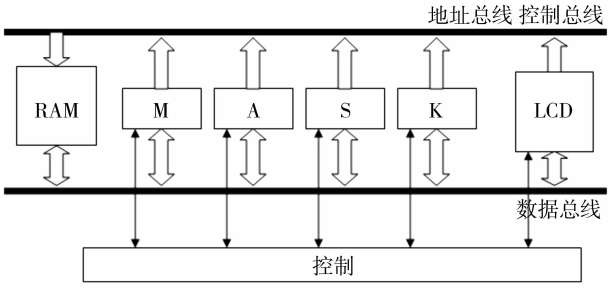

图 1　微控制/运算模块架构

RAM 模块仅有一个 PE 大小的数据空间，存储每个元素的值。通过读写控制线来决定操作，读信号来时，从地址线读取地址，取出 RAM 中的数据放到地址线上；写信号来时，将数据线上的数据写入地址线对应的位置。读写控制线都是由外部模块控制的。

整个数据流的走向如下：

1）显示原始数据。控制模块启动 LCD 模块的使能信号；LCD 模块初始化，并将数据从 RAM 中读出写入 LCD 液晶显示器的 DRAM 中。

2）加密操作。控制模块依次启动 M、A、S 和 K 模块的使能信号；在加密模块内部，先从 RAM 中读取要加密的数据，将加密后的数据存入 RAM，最后返回一个操作完成信号给控制，以便启动下一模块。

3）一轮加密结束操作。若是所有加密轮数完成，控制模块在得到全部加密完成的返回信号后，启动 LCD 模块的使能信号，将 RAM 内数据显示在液晶显示器上。若是还未完成所有的加密轮数，回到 2 步骤。

如前所述，解密步骤与加密步骤是相反的，因此在解密时需要控制模块发出一个解密信号指示各个模块加密操作与解密操作的区别，并控制基本操作的顺序，并不需要修改 4 个基本模块，通过这种方式可以大大节省 FPGA 实现所需的资源。

2.2　系统的实现

整个系统是在 QuartusII 5.1 开发平台上用 VHDL 硬件描述语言开发，并使用 ModelsimSE v6.0 软件模拟仿真，最后下载到 Cyclone EP1C60240C8 芯片上的一个完整的二值图像加密系统。

在各个模块的设计中，M 与 A 模块的运算主要运用了“＋”操作，在硬件实现中，“＋”操作选择用整数的按位 XOR 运算来实现。

S 模块是以数据的值为地址找到 Sbox 内的新值来替换旧值，所以并没有复杂的操作，值得注意的是，二值图像是以一个位为像素单位，每位只有 0 或 1 两种选择，此设计所选择的是 16×16 每单元 8 位的 Sbox[10]，所以需要将 PE 中的 8 个像素作为一个数据来置换 Sbox 内的一个新数据。如果所用到的显示器是支持 256 级灰度图像的，则只需要将每个象素作为一个数据来进行 Sbox 变换。

K 模块起到的是置乱功能，将 PE 中的某个单元从一个位置通过 K 映射的算法放到另一个位置上去。根据公式(5)，此算法使用到了“＋”、“－”、“×”、“/”和“mod”运算。然而后三种运算在硬件中属于高消费运算，即占用相当大的处理时间，在硬件设计中应尽量避免。在设计中，根据 K 映射的特殊性，可以将 PE 中以 O 划分的，n_s 长、P_s 宽的块映射到新 PE 中的一行中[2]。当 O 确定时，每个元素映射的位置就可以确定，而不需要付出高消费的运算。此系统中所用的 $O=(4,4,4,4,\cdots,4)$，简化了运算。

3　加密系统的评估

3.1　实验结果

图 2 显示了 32×32 的原始图像经过各个加密变换后的结果。

图 2　原始图像变换结果

多轮加密的结果见图3($MASK_i$ 代表第 i 轮加密的结果)：

(a)$MASK_2$ (b)$MASK_3$ (c)$MASK_4$

图3 多轮加密结果

从加密结果来看，密文呈现很强的随机性。

3.2 算法安全性评估

本设计是基于二值图像的加密，而大多数的对加密算法的评估是针对灰度图像而言，如直方图分析，但对于二值图像来说讨论直方图没有意义。所以通过讨论相邻象素的相关系数及UACI来说明算法能很好的淡化图像的相关性及有很好的扩散性。

3.2.1 相邻象素的相关系数

图像的一个显著特征是相邻象素的相关性很高，对一个象素而言，与之关联最紧密的是在水平、垂直和对角上相邻的象素，一般来说，在灰度图像中，相邻象素之间大多灰度值相近，在二值图像中，相邻象素相同的概率很高。一个成功的图像加密算法应该去除这种相关性，随机从PE中抽取500个象素点，分别从H(水平)、V(垂直)和B(对角)方向上计算明文和不同轮数的密文相邻相素的相关系数，对比结果见表1。

表1 明文和多轮密文相邻象素的相关系数

轮数	明文	1	2	3	4
H	0.743	−0.026 5	0.015 7	0.036 6	0.063 9
V	0.800	0.220 3	0.036 0	0.009 2	0.032 1
B	0.591	−0.104 8	−0.012 1	−0.020 6	0.047 6

可以发现，明文内相邻象素很强的相关性被加密算法淡化，到达第二轮加密之后，显稳定趋势，说明此算法很好地消除了象素相关性。

3.2.2 UACI分析

UACI(unified average changing intensity)，当原始图像有一位改变后加密的密图与原始图像对应的密图之间的差异如表2所示。

表2 多轮UACI比较

轮数	1	2	3	4
UACI	0.018 6	0.112 3	0.419 9	0.502 0

从表2可看出，当仅加密两轮时，密图之间仍有相当高的相似程度，4轮之后，密图之间的相似程度大大降低，达到相互独立。根据以上的分析，此算法在4轮加密及以上时，有很好的安全性。

3.2.3 其它安全问题

提出的算法中，Kolmogorov变换是公开的，并不依赖于密钥，其主要功能是在将局部的变换扩散到整个图像。系统的安全性主要依赖于A变换，即图像与密钥的异或操作。研究中使用的是32×32 dB的二进制流，密钥空间达到了2^{1024}，具有非常高的安全性。

3.3 系统性能评估

选用modelsim6.0对本系统进行功能仿真，在Quartus II下进行综合，最后下载到Cyclone EP1C60240C8芯片上，综合如表3。

表3 各模块所占资源

块	逻辑单元	引脚	存储位
M	148	29	0
A	114	29	0
S	241	29	0
K	2 848	29	0
RAM	0	25	1 024
控制	89	12	0
LCD	1 583	33	0

由表3可以看出，4个基本操作中M、A、S都是低耗能操作，而K变换占用相对较多的能源，这是跟操作本身相关。K操作是对一个PE进行置乱，所以K模块内部维持了一个暂存PE大小的存储空间，针对明文中的每一位，需要计算出置换的位置，即使采用固定的映射位置，也相当耗能。

从综合报告表4来看，复杂的加密系统MASK占用了较少的逻辑单元及存储空间，非常适用于低端便宜的FPGA。

表4 **MASK**加密系统资源消耗

资源类型	所用资源数/硬件资源数	所用资源/硬件资源/%
总逻辑单元	5 026/5 980	84
总引脚数	15/185	8
总存储位	1 024/92 160	1
总PLLs	0/2	0

4 结　论

提出了一种适用于硬件实现的离散混沌图像加密算法，并在 FPGA 上实现了该算法。首先介绍了该算法的加密解密过程和 4 个基本变换，并分析了该算法适宜于 FPGA 实现的特点。随后设计了对应于该算法的主要功能模块及相应的输入、输出和控制模块，并在 Cyclone EP1C6 芯片上实现了一个完整的图像加密系统。该文最后分析了算法的安全性及系统性能。实验证明，该系统安全性高，加密速度快，硬件资源消耗小，非常适宜于低端 FPGA 开发。

参考文献：

[1] LIAN S, SHUN J, WANG Z. A block cipher based on a suitable use of the chaotic standard map[J]. Chaos Soliton & Fractals, 2005, 26 (1):117-129.

[2] NECHVATAL J. Report on the development of the advanced encryption standard[J]. National Institute of Standards and Technology, 2000,10:201-203.

[3] PICHLER F, SCHARINGER J. Ciphering by Bernoulli shifts in finite abelian groups [J]. Contributions to General Algebra. Proc. Linz-Conference, 1994:465-476.

[4] SCHAROMGER J. Fast encryption of image data using chaotic Kolmogorov flows[J]. Journal of Electronic Imaging, 1998, 7(2): 318-325.

[5] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps[J]. I J Bifur Chaos, 1998, 8(6):1259-64.

[6] CHEN G, CHEN Y, LIAO X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps[J]. Chaos, Solitons & Fractals, 2007: 31(3), 571-579.

[7] TANG G P, LIAO X F, CHEN Y. A novel method for designing S-boxes based on chaotic maps[J]. Chaos, Solitons & Fractals 2005:23:413-9.

[8] KOHDA T, TSUNEDA A. Statistics of chaotic binary sequences [J]. IEEE Transactions on Information Theory, 1997, 43(1):104-12.

[9] CHEN G, MAO Y, CHUI C. Symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons & Fractals, 2004, 21 (3): 749-761.

[10] TANG G P, LIAO X F. A method for designing dynamical S-boxes based on discretized chaotic map[J]. Chaos, Solitons & Fractals 2005,23:9-1901.

[11] QI D, ZOU J, HAN X. A bew cass of scrambling transformation and Its application in the image information covering[J]. Science China, 2000, 43(3): 304-312.

[12] ZHANG M, Shao G, ANDYI K. T-matrix and its applications in image processing [J]. Electronics Letters, 2004, 40(25): 1583-1584.

[13] MANICCAM S, BOURBAKIS N. Image and video encryption using SCAN patterns [J]. Pattern Recognition, 2004, 37(4): 725-737.

[14] LIN C J, TSAI H M. FPGA implementation of a wavelet neural network with particle swarm optimization learning [J]. Mathematical and Computer Modelling, 2008, 47:982-996.

[15] FAIEDH H, GAFSI Z, TORKI K, BESBES K. Digital hardware implementation of a neural network used for classification[J]. International Conference on Microelectronics, 2004(12):551-554.

[16] MAEDA Y, TADA T, FPGA implementation of a pulse density neural network with learning ability using simultaneous perturbation[J]. IEEE Transactions on Neural Networks, 200314 (3) : 688-695.

（编辑　侯　湘）

(上接第 1188 页)

[12] WONG C. Multiuser OFDM with adaptive subcarrier, bit, and power allocation[J]. IEEE Journal on Selected Areas in Communications, 1999,17(10):1747-1758.

[13] QIU Y H, PAN Y H. Adaptive bit and power allocation with adaptive transmit diversity for broadband MISO/OFDM wire less transmission [C] // Neural Networks and Signal Processing. New Jersey: Proceedings of the 2003 International Conference, 2003(2):1472-1476.

[14] HU Z P, ZHU G X, XIA Y, et al. Adaptive subcarrier and bit allocation for multiuser MIMO-OFDM transmission [C] // Vehicular Technology Conference 2004. [s. l.]: VTC 2004-Spring, 2004(2):779 -783.

[15] TU J C, CIOFFI J M. A loading algorithm for the concatenation of codes with multi-channel modulation methods[J]. IEEE Globecom, 1990:1183-1187.

（编辑　侯　湘）