

一种新的图像自适应并行加密算法

刘祝华, 袁 文

(江西师范大学 物理与通信电子学院, 江西 南昌 330022)

摘 要: 提出了一种新的图像自适应并行加密算法. 该算法根据奇偶加密轮次对图像进行水平或垂直分组, 再对分组进行子块划分, 并使用相邻块像素扰动混沌映射, 同时设计了新的分组扩散方法, 并使用 S 盒完成像素非线性替代. 实验结果表明, 新算法具有安全、简单、高效的特点, 适合并行实现.

关键词: 图像加密; 自适应; 并行加密; 密码学

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2015)01-0068-04

A New Self-adaptive Parallel Image Encryption Algorithm

LIU Zhu-hua, YUAN Wen

(Physics and Communication Electronic College, Jiangxi Normal University, Nanchang 330022, China)

Abstract: A new self-adaptive parallel image encryption algorithm is proposed. In the new algorithm, image is divided into horizontal or vertical groups according to encryption rounds, each group is divided into two sub-blocks, chaotic mapping of each sub-block is disturbed by adjacent sub-block pixels, a new pixel diffusion method is designed, and pixels are replaced by using S box. The experiments show that the new algorithm has the advantages of safety, simple and efficient, which is suitable for parallel implementation.

Key words: image encryption; self-adaptive; parallel encryption; cryptography

1 引言

图像是网络信息传输的主要内容之一, 但传输过程中的非法盗用对图像信息安全影响很大^[1], 因此对图像进行加密保护也就显得越来越重要. 图像加密的方法很多, 而混沌具有天然的类噪声特性, 同时对系统参数和初始条件非常敏感^[2-4], 因此被广泛应用到图像加密算法设计中.

采用混沌系统的图像加密算法, 通常是使用混沌系统生成实数序列, 再根据算法的需要量化成不同范围的整数加密序列, 并作用于图像完成加密, 而作用的规则必须是可逆的^[5]. 在加密序列生成方法及作用于图像的规则上, 许多研究者提出了众多设计方案^[6-10], 但都具有类似的加密结构^[11], 即先对图像进行像素位置置乱, 再对每个像素值进行扩散加密, 而扩散过程往往是对每个像素逐一串行进行, 类

似 CBC 的加密模式. 而为了提高算法安全性, 置乱与扩散加密往往需要反复多轮, 因此图像加密的数据运算量很大, 加密时间往往也很长. 并行模式可以有效地提高运算速度, 文献^[12]提出了一种并行加密模型, 并分析了并行加密算法应该满足的条件, 即具有良好的扩散性能, 并保证各个 PE (Processing Elements) 之间计算负载的平衡, 以及实现 PE 之间数据通信的临界区域管理.

Zhou 等人^[12]中提出了一种并行图像加密算法, 对图像进行水平分组, 每个分组使用 AES 算法加密, 然后分组间采用 K (Kolmogorov flow) 变换进行像素重排, 并且进行多轮加密, 由于 K 变换涉及多次乘法运算, 因此算法耗时较长. Miraei 等人^[13]提出了将图像分成四个子图并行加密的算法, 但各子图独立加密, 也不存在像素重排, 因此扩散性能较差. 孙劲光等人^[14]提出了一种改进的图像分块加密

收稿日期: 2014-03-23; 修回日期: 2014-05-17

基金项目: 国家自然科学基金项目(11264016); 江西省教育厅科研基金项目(GJJ12172); 江西师范大学科研基金项目(4554)

算法, Wang 等人^[15]提出的算法, 设置了一组二进制序列, 每一轮加密时根据序列的值, 对图像按水平或垂直方向进行分组, 每个分组使用混沌映射生成的遍历矩阵实现像素位置置乱, 再使用相邻像素异或实现像素扩散, 由于扩散方式设计不合理, 存在扩散盲点, 并且置乱过程要进行大量数值矩阵排序, 增加了加密时间。

本文设计了一种按加密轮次交替改变图像分组方向的自适应并行加密算法, 实验结果表明新算法具有更高的安全性和更快的加密速度。

2 自适应并行加密算法

2.1 算法描述

2.1.1 图像分组

假设大小为 $m \times m$ (m 为偶数) 的图像 P 由 r 个 PE 进行 l 轮并行加密, 且 m 能被 r 整除。奇数轮时, 对图像进行水平分组, 第 i 个 PE_i 负责分组 P_i 的加密, P_i 是原图像 $(i-1) \cdot \frac{m}{r} + 1$ 行到 $i \cdot \frac{m}{r}$ 行的内容; 偶数轮时, 对图像进行垂直分组, 第 i 个 PE_i 同样负责分组 P_i 的加密, 但 P_i 是 $(i-1) \cdot \frac{m}{r} + 1$ 列到 $i \cdot \frac{m}{r}$ 列的内容, 其中 $i \in [1, r]$ 。

2.1.2 分组加密

奇数轮时, 每个分组 P_i 左右划分成大小相等的两个子块 P_i^L 和 P_i^R 。对 P_i^L 加密时, 使用 Logistic 映射生成长度为 $\frac{m^2}{2r} + \frac{m}{r} + \frac{m}{2}$ 的混沌序列 X_i^L 。生成 X_i^L 时, 按式(1)对 Logistic 映射的参数 μ 和初始值 x_0 进行扰动,

$$\begin{cases} \mu = (key_1 + (3.9 + 0.1 \times t_0/255))/2, & key_1 \in (3.9, 4) \\ x_0 = (key_2 + t_1/255)/2, & key_2 \in (0, 1) \end{cases} \quad (1)$$

式中, t_0 和 t_1 为扰动参数, 分别由 P_i^R 的前两个像素 $P_i^R(1, 1)$ 、 $P_i^R(1, 2)$ 代入, key_1 和 key_2 为加密密钥。

将 X_i^L 的前 $\frac{m^2}{2r}$ 个元素量化成 $[0, 255]$ 的整数, 并转

换成 $\frac{m}{r} \times \frac{m}{2}$ 的加密矩阵 E_i^L 。将 X_i^L 的第 $(\frac{m^2}{2r} + 1)$ 至第 $(\frac{m^2}{2r} + \frac{m}{r})$ 个元素量化成 $[0, \frac{m}{2} - 1]$ 的整数, 得长

度为 $\frac{m}{r}$ 的序列 SR_i^L 。将 X_i^L 的第 $(\frac{m^2}{2r} + \frac{m}{r} + 1)$ 至第

$(\frac{m^2}{2r} + \frac{m}{r} + \frac{m}{2})$ 个元素量化成 $[0, \frac{m}{r} - 1]$ 的整数, 得

长度为 $\frac{m}{2}$ 的序列 SC_i^L 。按序列 SR_i^L 的值对 P_i^L 逐行循

环右移, 再按序列 SC_i^L 的值对 P_i^L 逐列循环下移, 实现 P_i^L 的像素置乱; 再与加密矩阵 E_i^L 的每个元素按位异或。按相同的方法对 P_i^R 进行加密, 此时用 P_i^L 加密后的前两个密文对 Logistic 映射的参数和初始值进行扰动。用 P_i' 表示加密后的分组。

为进一步提高算法抗差分攻击能力, 必须对 P_i' 进行扩散操作。文献[12]中采用 $c_i = p'_i \oplus (p'_1 \oplus p'_2 \oplus \dots \oplus p'_n)$ (n 为分组元素个数, c_i 为扩散后结果) 的方法实现分组内像素扩散, 这使得任意 c_i 都是除 p'_i 之外其他像素异或的结果, 若恰好 p'_i 有细微变化, 则不会扩散至 c_i , 算法存在扩散盲点, 影响了整个密文的扩散效果; 文献[15]中使用相邻像素异或实现像素扩散, 会使分组最后一个像素 $c_n = p'_1 \oplus p'_2 \oplus \dots \oplus p'_{n-1}$, 同样存在扩散盲点。因此, 本文设计了如下的扩散操作, 新的扩散操作使得分组中第一个像素的扩散结果是分组中所有像素值求和后对 256 取模的结果, 因此, 任意像素的变化都会扩散至第一个像素, 再经异或操作会扩散至整个分组, 很好地解决了文献[12, 15]存在扩散盲点的问题。最后, 再用 AES 加密标准中的 S 盒对分组中的每个结果进行非线性替代。

$$\begin{cases} C_i(1, 1) = (\sum_{u=1}^{\frac{m}{r}} \sum_{v=1}^{\frac{m}{2}} P_i'(u, v)) \bmod 256 \\ C_i(u, v) = P_i'(u, v) \oplus C_i(1, 1), \begin{cases} u = 1 \text{ 时}, v \in [2, m] \\ u \in [2, \frac{m}{r}] \text{ 时}, v \in [1, m] \end{cases} \end{cases} \quad (2)$$

偶数轮加密时, 方法与奇数轮相同, 但每个垂直分组按上下划分成大小相同的两个子块。

重复上述步骤, 直到完成 l 轮加密。上述所有操作步骤都是可逆的, 因此算法能够正确解密。

2.2 算法分析

加密时每个分组的每个子块都会用相邻子块的元素对其混沌映射的参数及初始值进行扰动, 因此每个子块的加密矩阵和置乱序列不仅和密钥有关, 而且与明文密切相关, 有效提高了算法抵抗选择明文和已知明文攻击的能力。算法采用循环移位实现像素位置置乱, 相比于文献[15]中的遍历矩阵法, 少去了大量加密序列排序的操作, 降低了像素置乱的复杂度, 提高了算法运行速度。

算法设计了新的扩散操作, 很好地解决了文献[12, 15]中存在扩散盲点的问题, 同时使用了加密矩阵异或和 S 盒替代, 其中 S 盒的非线性变换过程能有效增强算法抗线性和差分分析的能力。算法的扩

散操作、加密矩阵异或及 S 盒替代都是类似 ECB 的加密模式,相比于 CBC 模式,更加简单高效,便于并行实现.

算法奇数轮进行水平分组加密,偶数轮进行垂直分组加密,确保了明文任意像素的变化经两轮即可扩散至整个密文.另外,算法中每个 PE 的处理对象都是大小相同的分组,因此保证了各个 PE 具有相同的计算负载;而且,加密时每个分组之间不存在数据交换,因此不存在临界区域管理问题.本文算法能够满足图像并行加密算法的各项要求.

3 实验结果

实验采用 Intel 酷睿 i5 双核 2.4 GHz 的 PC 机模拟并行运行环境,在 Windows7 操作系统下使用 Matlab7.6 编写测试程序.明文图像使用 512×512 的 Man 灰度图,密钥取 $key_1 = 3.902, key_2 = 0.002, PE$ 数 $r = 16$.实验要对算法的安全性能与运行速度进行测试,并与文献[12, 15]算法进行比较.

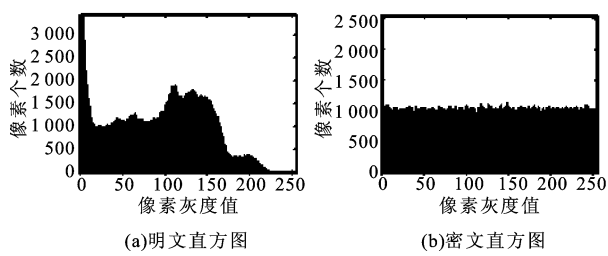
3.1 抗统计攻击性能分析

对 Man 图像进行 2 轮加密,效果如图 1 所示,而图 2 给出了加密前后明、密文的直方图结果.从图 1 的结果可以看出加密后密文中反映不出原图像的任何信息.



(a)明文图像 (b)密文图像

图 1 Man 图像加密效果



(a)明文直方图 (b)密文直方图

图 2 Man 图像加密前后的直方图

从图 2 的直方图结果可以看出密文图像的灰度分布十分均匀,从而很好地掩盖了原图像灰度分布的情况.也可用信息熵来衡量图像中灰度值的分布

情况,图像灰度分布越均匀,则信息熵越大,反之越小.对于 256 级灰度图,信息熵最大值为 8.原 Man 图像信息熵为 7.192 6,以上述初始密钥为起始值,按 0.000 001 步长,连续微调密钥 key_1 100 次,计算密文图像信息熵均值为 7.999 3,非常接近最大值 8,调整密钥 key_2 可以得到类似结果.从直方图和信息熵分析可知,本文算法的密文图像灰度分布十分均匀,能有效抵抗统计攻击.

3.2 扩散性能分析

明文图像的细微变化会导致密文图像的改变,攻击者可以从中找到某种规律从而破译算法.如果算法的扩散能力很强,明文微小的变动会导致密文非常大的变化,那么这种攻击就难以实现.算法的扩散能力可以通过密文比特改变率来衡量,当明文改变一个比特位时,应该有接近 50% 的密文比特位发生变化.将 Man 图像最后一个像素的最低位取反,表 1 列出了各轮加密后密文的比特改变率.由于第一轮最后一个像素的变化只在最后一个水平分组扩散,因此,比特改变率只有 0.030 8.但经过第二轮垂直分组加密后,像素的变化扩散至整个密文,比特改变率升至 0.504 3,而且之后一直保持在 0.5 左右,表明算法扩散性能很好.

表 1 明文改变一位后的密文比特改变率

轮次	1	2	3	7	8	9
改变率	0.030 8	0.504 3	0.499 9	0.500 1	0.500 3	0.500 0

3.3 密钥敏感性分析

算法应该对密钥的变化非常敏感,密钥的微小改变应该产生完全不同的密文结果.微调密钥 key_2 ,加上 10—15,对比加密后密文的变化,表 2 列出了各轮加密后密文的比特改变率.从表 2 可以看出,密文的比特改变率一直保持在 0.5 左右,表明算法对密钥的变化非常敏感.

表 2 微调密钥后的密文比特改变率

轮次	1	2	3	7	8	9
改变率	0.500 1	0.500 0	0.499 8	0.500 1	0.500 4	0.499 9

3.4 相关性分析

原图像相邻像素相关性很高,加密后应该很好地去掉这种相关性.相关系数^[9]反映了相邻像素之间的相关性,其值越接近于 1,则相邻像素相关性越高,越接近于 0,则相关性越低.计算 2 轮加密前后水平、垂直和对角三个方向相关系数,如表 3 所示.密文图像三个方向相关系数都非常小,说明本文算法经两轮加密就能很好地破坏相邻像素的相关性.

使密文呈现随机性分布.

表 3 相邻像素相关系数

方向	明文	密文
水平	0.956 6	0.002 9
垂直	0.939 9	0.001 7

3.5 与同类算法的比较

将本文算法与文献[12,15]中的算法进行比较.在安全性方面,本文算法要优于文献[12,15]中的算法.文献[12]中存在扩散盲点,而且分组间使用 K 变换进行像素重排,需要至少三轮才能实现整个密文扩散;另外,分组内没有像素置乱操作,加密过程也没有明文介入,存在安全隐患.文献[15]中同样存在扩散盲点,而且置乱操作只与混沌映射生成的数值矩阵有关,与明文无关,容易受到已知明文攻击;另外,算法设置了二进制密钥序列 $b_1, b_2, \dots, b_n$,若 b_1 开始出现连续多个 0 或连续多个 1,会使 PE 连续多轮进行水平或垂直分组加密,从而影响整个密文的扩散效果.

在加密速度方面,表 4 列出了三种算法加密同一图像(512×512 的 Man 灰度图,16 个分组,加密 10 轮)的时间对比结果,可以看出本文算法要明显优于文献[12,15]中算法.主要是因为文献[12]中算法分组间每个像素的 K 变换涉及多次乘法运算,而乘法运算要比异或和置换操作慢得多.而文献[15]中算法分组内的置乱操作,需要对加密序列进行排序,通常其最低时间复杂度为 $O(\frac{m^2}{r} \cdot \log \frac{m^2}{r})$,耗费时间较长.另外,本文算法采用了 ECB 的加密模式,也进一步提高了加密效率.

表 4 三种算法的加密时间

加密算法	文献[12]	文献[15]	本文算法
加密时间/s	2.076 3	1.172 7	0.404 3

4 结束语

本文提出了一种新的图像自适应并行加密算法,提出:(1)奇数轮进行水平分组,偶数轮进行垂直分组;(2)每个分组按左右(或上下)划分大小相等子块,每个子块用相邻块像素扰动混沌映射,生成加密矩阵和置乱序列;(3)每个子块根据置乱序列,使用行、列循环移位实现像素置乱,并用加密矩阵异或实现子块加密;(4)使用新的扩散方法(式(2))实现像素扩散,并使用 S 盒完成像素的非线性替代.通过实验比较表明新算法在安全性和加密速度上都要明显优

于文献[12,15]算法.

参考文献:

- [1] Ma X, Fu C, Lei W M. Novel chaos-based image encryption scheme with an improved permutation process [J]. International Journal of Advancements in Computing Technology, 2011, 3(5): 223-233.
- [2] Lu H P, Wang X W. A new spatiotemporally chaotic cryptosystem and its security and performance analyses [J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2004, 14(3): 617-629.
- [3] Yang Y, Liao X F. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map [J]. Physics Letters A, 2007, 363(4): 277-281.
- [4] Wang Z Z, Han Q Y. Finite-time chaos synchronization of unified chaotic system with uncertain parameters [J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(5): 2239-2247.
- [5] Kocarev L, Maggio G M, Ogorzalek M, et al. Special Issue on application of chaos in modern communication systems [J]. IEEE Transaction on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(12): 1394-1404.
- [6] 唐宋, 徐桂兰, 李清都. 基于高维超混沌系统和矩阵张量积的图像分组加密新算法[J]. 计算机应用, 2012, 32(8): 2262-2264.
- [7] 郭晓丛, 向菲, 刘伟. 一种基于多混沌映射的图像加密算法[J]. 计算机工程, 2012, 38(20): 93-96.
- [8] 王阳, 吴成茂, 梁睿. 基于混沌选择的自适应图像加密算法[J]. 微电子学与计算机, 2013, 30(5): 132-136.
- [9] 文昌辞, 王沁, 黄付敏, 等. 基于仿射和复合混沌的图像自适应加密算法[J]. 通信学报, 2012, 33(11): 119-127.
- [10] 吴新华. 基于混沌的位级图像加密算法研究[J]. 微电子学与计算机, 2013, 30(12): 69-72.
- [11] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map [J]. Communications in Nonlinear Science and Numerical Simulation, 2012, 17(7): 2943-2959.
- [12] Zhou Qing, Wong Kwokwo, Liao Xiaofeng, et al. Parallel image encryption algorithm based on discretized chaotic map [J]. Chaos Soliton & Fractals, 2008, 29(11): 1081-1092.
- [13] Omid Mirzaei, Mahdi Yaghoobi, Hassan Irani. A new image encryption method: parallel sub-image encryption with hyper chaos [J]. Nonlinear Dynamics, 2012, 67(1): 557-566.

(下转第 75 页)

(4) 根据目标体系结构硬件特性,对 GDB 前端进行相应的修改以使得 GDB 的某些功能可以正常运行,如读写内存、变量等。

(5) 添加新的用户命令及机器命令,为用户及机器调用留下多核调试功能接口。

(6) 扩展 RSP 协议,以满足上面提到的多核调试新的功能要求。

4.2 调试代理的设计实现

调试代理作为调试器与目标板的中介,需要负责连接多个调试器,处理它们并发的调试请求,通过 RSP 协议解析调试命令,控制硬件完成调试操作,再将正确的结果回传。具体应该实现的功能如下所示。

(1) 调试代理需要作为一个并发服务器实现。系统以进程的形式逐个启动调试器,并向调试代理发起连接。调试代理必须能正确处理它们的并发连接以及调试请求。此外,调试代理对目标 DSU 的控制接口作为唯一资源,为多个调试器所共享,其间的互斥工作也必须处理妥当。

(2) 调试代理需要正确的解析 RSP 协议中相关命令以及扩展命令,并控制硬件完成相应的操作,将结果返回给用户。能让 GDB 运行的最小 RSP 命令集合为 g、G、m、M、c,其具体含义可见上文对 RSP 协议的讨论。

(3) 调试代理需要准确的识别出调试请求由哪一个调试器发出,并控制相应的处理器核完成相应的调试操作再将结果回传。硬件方面,由于各处理器核的内存结构完全相同,仅由地址空间区分。因此,在接受调试器连接时,可为该进程编号,这样,便很容易得出调试器与相应处理器核的映射关系,从而进行正确的操作并返回结果。

(4) 调试代理需要提供全局统一的控制接口,以使所有的处理器核同时运行或停止。多核调试,各核之间的同步非常重要,能对其进行统一的控制,便可以使调试态与运行态保持一致,从而得到更为准确的调试结果。调试代理可以通过依次控制各个调试器操作相应

的处理器核来实现这样的功能。然而,这样的方法必然有调用延迟,实时性差。如果硬件支持的话,可以采用先通过硬件手段同时停止所有处理器核,再将调试器所需要的调试信息回传给各个调试器的方法。

5 结束语

本文针对多核 DSP 平台 LCSA3201A,结合 GDB,设计实现了一种能满足主流调试要求的源码级多核调试系统。该系统实现简单、可靠性好,但同时占用系统资源较多。不过,多核调试技术依然在不断的完善和发展中,只要对调试代理进行相关的完善和升级,必然能实现更好更强的调试环境。

参考文献:

- [1] 贺松建. 多核处理器技术浅析[J]. 科技促进发展, 2009(2):60-63.
- [2] 刘洋,张毓森,甄奇. 基于 GDB 的 ARM 嵌入式调试系统的设计与实现[J]. 军事通信技术, 2007, 28(Sup): 22-28.
- [3] Bill Gatloff. Embedding with GNU: the gdb remote serial protocol[J]. Embedded Systems Programming, 1999(9):109-116.
- [4] 杨文博. GNU Debugger 的移植及原理分析[D]. 南京: 南京大学, 2007.
- [5] Jeremy Bennett. Howto: porting the GNU Debugger—Practical Experience with the OpenRISC 1000 Architecture[J]. Embedded Software Development, 2008, 2(3):1-74.

作者简介:

李琮 男, (1989-), 硕士研究生. 研究方向为计算机应用技术. E-mail: lc19890709@126.com.

王竹平 男, (1963-), 研究员, 总工程师. 研究方向为嵌入式计算机软硬件设计.

费晓琪 男, (1972-), 高级工程师. 研究方向为嵌入式计算机软件设计.

(上接第 71 页)

- [14] 孙劲光, 汪洁, 姜文涛, 等. 改进的分块算法在矩形图像加密中的应用[J]. 计算机应用研究, 2013, 30(1): 282-284.
- [15] Jing Wang, Guoping Jiang. A self-adaptive parallel encryption algorithm based on discrete 2D-logistic map [J]. International Journal of Modern Nonlinear Theory and Application, 2013(2): 89-96.

作者简介:

刘祝华 男, (1977-), 硕士, 讲师. 研究方向为信息安全、数字图像处理等. E-mail: happy_lzh@126.com.

袁文 男, (1972-), 博士, 教授. 研究方向为信号检测与处理.