多核处理器降低功耗技术综述*)

郝 松[1] 都志辉[1] 王 曼[1] 刘志强[2]
(清华大学计算机系 北京 100084)[1] (河北大学科技处 保定 071000)[2]

摘 要 随着芯片集成度越来越高,处理器功耗已经和性能、时钟频率、芯片尺寸共同成为衡量一个处理器优劣的最主要标准。传统的降低功耗的技术都是针对功耗本身,即动态消耗和静态消耗,针对动态消耗的有多元供能电压技术(Multiple Supply Voltage)、动态电压调节技术(Dynamic Voltage Scaling)和基于时钟信号的技术,针对静态消耗的有通道长度调整技术(Channel Length Scaling)、寄存器锁存技术和能量选通技术(Power Gating)。近两年从处理器结构和算法角度思考降低功耗逐渐成为热点,在未来一段时间将成为研究的主要方向。

关键词 动态消耗,静态消耗,结构和算法优化

Survey on Multi-core Processors Power Consumption Reducing Technologies

HAO Song[1] DU Zhi-Hui[1] WANG Man[1] LIU Zhi-Qiang[2]
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084)[1]
(Science and Technology Office, Hebei University, Baoding 071000)[2]

Abstract With the increasing in chip density, power consumption, together with performance, clock rate and chip area, has become the prime criterions to evaluate a processor. Traditional technologies mostly focus on the consumption itself including dynamic and static consumption. Most of these technologies have already been widely used. Multiple supply voltage, dynamic voltage scaling and clock gating are used to reduce dynamic consumption. Channel length scaling and power gating are used to reduce static consumption. Power consumption reducing from optimizing the processor architecture and algorithm has become a hot pot, and will be the main direction in this field.

Keywords Dynamic consumption, Static consumption, Architecture and algorithm optimization

1 引言

随着半导体技术的进步,处理器的集成度迅速提高,带来了性能和速度的提升,但同时处理器的能耗也大幅度增加了,这意味着释放更多的热量。对此,生产厂商不得不采用更高效的冷却措施,但无疑将增加成本。目前,处理器的设计已经由单核转向多核,而多核处理器存在着发热大、散热难的问题。另外,随着手提设备的普及,延长电池单次充电的使用时间成了广大客户的共同需要。虽然电池技术的发展对于化学工业来说已经相当快了,但仍然赶不上处理器的发展和应用的需求。基于上述原因,降低处理器的功耗成了当务之急。

本文就目前存在的降低处理器功耗的技术和方法进行阐述和分析。第2部分将简述降低功耗技术的发展、评价标准。第3,4部分将分别介绍降低动态消耗和静态消耗的技术。第5部分讨论如何通过非对称多核处理器结构降低功耗。第6部分介绍针对冗余多线程的优化算法。最后给出总结和展望。

2 降低处理器功耗技术概述

2.1 降低功耗技术的发展

处理器功率的消耗主要来自三个方面[1],总功耗可以表示如下:

$$P_{avg}=P_{short}+P_{dyn}+P_{static}$$

其中 P_{short} 为电路的短路功耗,它是晶体管在逻辑门打开的瞬间同时产生的,这部分功耗一般比较小。

动态消耗 P_{dyn} 包括处理器内部各元件正常工作时所消耗的电能,例如电容性的充放电、切换频率、逻辑门的状态转换等等。降低动态消耗一直以来都是人们研究的重点,而且技术比较成熟,比如动态电压调节、时钟屏蔽技术等等。

后来,随着静态消耗在全部功率消耗中所占比重的增加,人们开始重视静态消耗的降低。功率的静态消耗 P_{static} 是指来自漏电流的功率消耗,具体包括亚阈值漏电流和门漏电流。经过几年的发展,降低静态消耗的技术也趋于成熟。

最近两年,这种电路级的低功耗技术进展缓慢,通过优化处理器结构和算法达到降低功耗的目的将成为主要的研究方向。

2.2 EPI——功耗评价标准

EPI是衡量处理器能量效率的标准,它表示处理器平均执行一条指令需要消耗的能量。EPI的单位可以为Joules/instruction(焦耳/每条指令)或者是Watt/IPS(瓦特/每秒指令数)。EPI值越大,处理器的能源效率就越差。处理器的EPI决定因素有三个方面:设计(包括微架构、逻辑、电路、布线等等)、加工工艺和供电电压。

3 降低动态消耗的技术

3.1 多元供能电压技术(Multiple Supply Voltage)

*)国家自然科学基金(No. 60503090)、北京市自然科学基金(No. 4042,081)、973子项目(No. 2004CB217903)。**郝 松** 硕士,主要研究领域为网格计算;**都志辉** 博士、副教授,主要研究领域为网格计算、高性能计算。

单个晶体管的动态消耗可以用下面的公式表示：

$P_{dyn}=KCfV_{dd}^2$

其中，K 是状态转换因子，由晶体管的物理特性决定；C 是晶体管的装载电容；f 是时钟频率；V_{dd} 代表供能电压。由于动态消耗正比于供能电压的二次方，所以通过降低供能电压可以有效地减少动态消耗。但是过低的供能电压会对处理器的性能造成影响，解决这个问题的技术目前有两种：CVS(Clustered Voltage Scaling)技术和 RRPS(Row by Row optimized Power Supply scheme)技术。这两种技术都基于提供多元的供能电压思想，即对不同的功能部件提供不同的电压。

3.1.1 CVS 技术

CVS 技术是最早提出的通过提供多元供能电压来降低功率的技术之一，它将处理器内的逻辑电路分成两个组，即关键路径上的电路(处于系统的瓶颈部分，性能下降会引起整个系统性能的下降，如流水线、cache)和非关键路径上的电路(对处理器性能不产生决定性影响的部件)。降低非关键路径电路的电压从而降低其功耗，而关键路径上仍保持正常的工作电压以保证处理器的性能。

采用这种方法效率很高，可以降低处理器平均 47%的功耗，但是它的问题在于：这样人为的分组造成了两组电路之间较大的通信延迟，进而对处理器的性能产生影响。尤其在多核处理器中，如何选择分组的粒度，从而保持处理器内部互连网络的效率，成了 CVS 技术很难解决的问题。另外，由于需要增加额外的控制器件，所以造成芯片面积平均增加 15%。

3.1.2 RRPS 技术

与 CVS 的分组方式不同，RRPS 技术提供一种细粒度的多元供能电压的机制，其实质是为每个基本元件(例如缓冲器、锁存器)都提供不同的电压。

我们以时钟锁存器为例介绍 RRPS 技术的工作机制[12]。

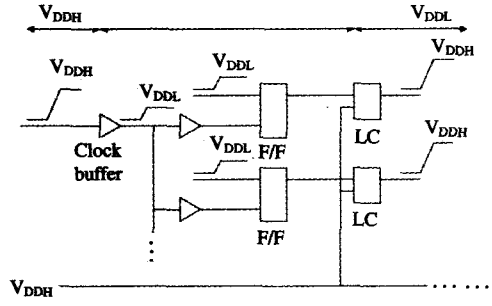

图 1 RRPS 技术在时钟锁存器的应用

在时钟锁存器(F/F)前面增加一个工作电压为 V_{DDL} 的时钟缓冲器，当峰值为 V_{DDH} 的时钟信号通过时钟缓冲器之后，峰值变为 V_{DDL}。由于时钟锁存器是边沿触发的，所以改变峰值不影响它的正常工作。当时钟信号通过时钟锁存器之后，进入一个电压变换器(LC)，使其恢复到 V_{DDH} 的峰值。

RRPS 技术由于采用了细粒度的多元电压机制，可以避免 CVS 技术中存在的通讯延迟，但它的不足是需要增加大量的供电线路才能使每个功能单元都能在两种电压之间选择，将增加硬件设计的复杂性。

3.2 动态电压调节技术(Dynamic Voltage Scaling, DVS)

动态电压调节[7]在多元供能电压思想的基础上提供了一种基于应用的电压管理方法，它根据应用程序对计算资源的需求程度动态地调整处理器的电压和时钟频率，从而在满足应用需求的基础上最大限度地降低功耗。

由于 DVS 技术要随时了解系统中应用程序对资源的需求情况，而处理器的硬件无法判断它所执行的程序的计算量，所以它需要操作系统的支持。操作系统根据当前所有任务的计算量，调节处理器的速度。处理器的速度可以通过调整时钟频率来调节，操作系统将所需的时钟频率传递给处理器中的电压调节系统，电压调节系统根据时钟频率计算出时钟振荡器所需的电压，并将该电压输出到时钟振荡器，从而控制处理器的速度。同时，电压调节系统要根据该时钟频率计算确保处理器正常运行而且功耗最低的供能电压，并将它输送到供电线路上。

动态电压调节技术能在满足程序运行要求的性能前提下来降低功耗。特别是当多核处理器不同核心上运行着的应用程序对速度的要求不同时，这种能力可以使得处理器总是运行在一个最优的能量效率比上，最大限度地节省功耗，在一些应用中甚至可以达到节省 80%的功耗[10]。但是它需要操作系统的支持，而且电压的调节过程需要一定时间，所以对处理器的性能有一定影响。

3.3 基于时钟信号的技术

3.3.1 时钟屏蔽技术(clock gating)

时钟屏蔽技术[5]的主要思想是对一段组合逻辑电路的时钟信号增加控制逻辑，当电路处于空闲状态时，截断该部分的时钟信号。其实质是通过控制时钟减少不必要的状态转换，从而降低动态消耗。

为了控制时钟信号，需要设计专门的逻辑来判断当前电路所处的状态，并根据不同的状态发出不同的控制信号，如图 2[6]所示。

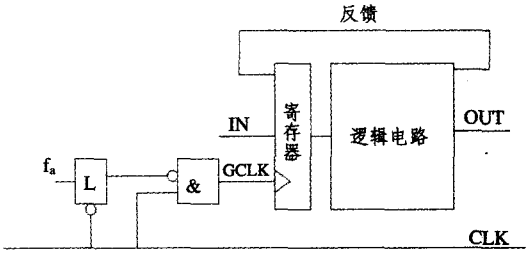

图 2 时钟屏蔽技术原理

判断逻辑判断电路所处的状态之后，发出控制信号 f_a，当 f_a 有效时，时钟信号进入所控制的逻辑电路，否则时钟信号将被屏蔽。

时钟屏蔽技术可以彻底解决动态消耗问题，应用十分广泛，例如 IBM power5 双核处理器、Intel Montecito 双核处理器。但它也存在不足，首先它需要增加复杂的判断逻辑，判断逻辑本身也消耗电能，而且如果出现判断错误的话，将造成电路失效，造成严重后果。

3.3.2 时钟树关闭技术

时钟树关闭技术可以降低时钟树本身动态消耗。有研究表明，时钟信号所消耗的电能占全部处理器所消耗电能的 15%～40%，时钟树关闭技术正是针对这种现象提出的一种降低时钟信号本身功耗的技术。其思想是对一段组合逻辑的时钟源增加控制逻辑，当组合逻辑处于时钟屏蔽状态时，控制信号同时关闭这个时钟源。

其工作机制见图 3。在采用时钟屏蔽技术的电路中，当

g1,g2 将时钟信号屏蔽之后,时钟信号仍然会在 b1,b2 段消耗电能。此时,如果在 b1,b2 之间加入一个时钟树的控制逻辑 r1,使它能将路径 b1,b2 上的时钟信号关闭,就可以消除 b1,b2 段的电能消耗。

时钟树关闭技术是对时钟屏蔽技术的扩充,可以降低时钟树的电能消耗,其不足在于:当采用时钟关闭技术的逻辑单元数量为 n 时,时钟树的边数在 $O(2^n)$ 数量级上,导致无法在所有时钟路径上增加控制单元。

3.4 降低动态消耗技术小结

表 1 总结、比较了降低处理器动态消耗的几种技术,各有优点和不足。其中,动态电压调节技术和时钟屏蔽技术是目前应用最多的,而且技术比较成熟。

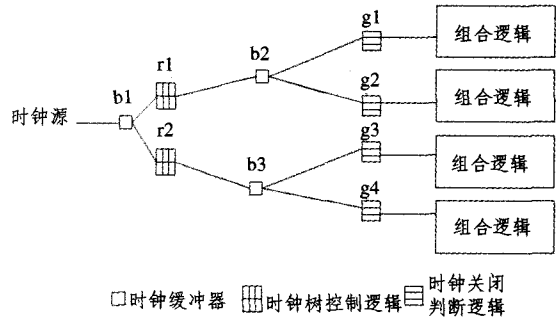

图 3 时钟树关闭技术

表 1 降低动态消耗技术总结比较

技术	优点	缺点	备注
CVS 技术	实现方法简单	电路组之间的通信延迟较大,影响处理器效率	针对处理部件和电路的电压调整技术
RRPS 技术	不需要对电路分组,消除了通信延迟	需要增加大量的供电线路,增加了芯片设计的复杂性	提供一种细粒度的多元供能电压
动态电压调节	能在满足程序运行所要求的性能前提下来降低功耗,使得处理器总是运行在一个最优的能量效率比上,最大限度的节省功耗	需要操作系统支持;电压调节需要一定时间,影响处理器效率	是应用最广泛的降低动态消耗的技术
时钟屏蔽技术	能彻底的消除动态消耗	对硬件依赖性很大,如果出现判断错误,后果严重	思想提出很早,应用广泛
时钟树关闭技术	消除了时钟树本身的动态消耗	问题的规模在 $O(2^n)$ 数量级,很难在每条时钟路径上都应用	是对时钟屏蔽技术的补充

4 降低静态消耗的技术

静态消耗是指来自漏电流的功率消耗,特点是即使元件处在空闲状态也会消耗电能。

4.1 通道长度调整(Channel Length Scaling)

通道长度调整是一种通过优化芯片的制造工艺来达到减小亚阈值漏电流的方案。亚阈值漏电流是一种贯穿晶体管的微弱电流,它可以通过延长晶体管的导电通道来减小,但这样做会带来一定的延迟。图 4[3] 反映了漏电流的强度随通道长度变化的情况。

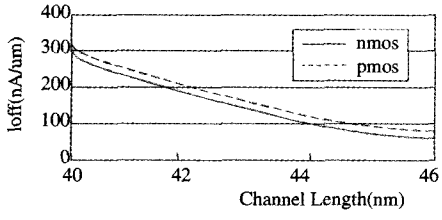

图 4 晶体管通道长度变化对漏电流强度的影响

在 $T=85℃$、$V_{dd}=1V$ 时,无论 nmos 晶体管还是 pmos 晶体管,将通道长度由 40nm 增加到 45nm,都可以使漏电流从 300nA/μm 降低到 90nA/μm。但通道长度的增加会使晶体管开关充放电的时间增加,对性能产生影响。实验证明,在通道长度增长为 45nm 时,静态消耗会减少 20%,但会带来 5%的速度损失。另外,增加通道长度还会导致处理器动态消耗的增加,这也是它的缺点。

4.2 寄存器锁存技术

寄存器锁存技术是降低静态消耗的一种常用方法,其思想是当处理器中的一个功能部件不处于工作状态时,将这个部件中主要寄存器的数据复制到低功耗的锁存器中,并切断该功能部件的供电电压。当功能部件需要恢复工作时,再将数据从锁存器复制回寄存器,从而达到降低功耗的目的。

Anantha Chandrakasan 等人通过实验证明,亚阈值漏电流的强度可以用如下公式[4]表示:

$$I_{sub}=K_1 W e^{-V_{th}/nV_\theta}(1-e^{-V/V_\theta})$$

可见,当其他参数不变时,增加阈电压 V_{th} 可以减小亚阈值漏电流。所以,通常采用掺入杂质的方法使锁存器的阈电压高于功能部件中寄存器的阈电压,来降低锁存器中的静态消耗。

寄存器锁存技术由于其实现方法简单,不需要增加过多的控制逻辑而被广泛采用,但其不足在于:由于采用较高的阈电压,锁存器的状态转换需要较长时间,所以不宜用在处理器的关键部件上,否则会影响处理器的速度。

4.3 能量选通技术(Power gating)

能量选通技术[2,5]是通过切断晶体管的供能电压来消除漏电流。有研究表明,在处理器运行期间,多数功能单元在相当大比重的时间内处于空闲状态。能量选通技术正是基于这种现象,切断暂时空闲的功能单元的供能电压,减少不必要的能量消耗。

与单核处理器不同,在多核处理器中,能量选通技术既可以用在基本的功能单元上,也可以用在整条流水线、核心等较高的层次上。

能量选通技术的优势在于抓住了处理器硬件资源不能被完全利用的特点,有效地减少了消耗电能的元件数量。但是它还存在着不足:首先,检测电路的存在增加了硬件设计的复杂性,而且带来了额外的能耗;另外,供能电压从 V_{CC} 降到 0

和从0重新升到V_{CC}都需要几个时钟周期，所以只有功能单元将长时间处于空闲状态时才可以应用能量选通技术，这限制了它的应用范围。

4.4 降低静态消耗技术小结

表2总结了各种用于降低处理器静态消耗的技术及其优缺点，其中能量选通技术(Power Gating)目前应用最为广泛，其思想还可以用于降低动态消耗的领域。

表2 降低静态消耗技术总结比较

技术	优点	缺点	备注
通道长度调整技术	能从根本上解决静态消耗问题；易于实现	影响处理器性能；还会增加动态消耗	在晶体管的制造工艺上优化处理器功耗
寄存器锁存技术	可以降低一些暂时不工作但未来一段时间将要继续工作的器件功耗	需要较多的硬件逻辑来实现；不能应用在关键路径上	通过缓存寄存器数值的方式，将器件解放出来
能量选通技术	可以有效减少空闲器件的能耗，能运用在处理器的各个功能部件上	需要增加复杂的硬件逻辑；器件恢复工作需要较长时间，影响处理器的效率	目前应用最广泛的技术之一

5 非对称多核处理器

上面介绍的降低动态消耗和静态消耗的技术在单核时代便已经出现，在多核处理器中也被广泛采用。而这部分介绍的非对称结构和下一部分将介绍的改进RMT技术则是多核处理器出现之后，从处理器结构和算法角度对能耗进行优化的方法。

非对称多核处理器的发布最初是基于这样的原因：服务器端的应用程序重视单位时间的吞吐率，为满足这种需要，处理器中应该集成较多数目的功能简单得核心；而PC机的用户更关注一个或少量几个应用程序的响应时间，满足这种需要的处理器应该只集成几个功能强大的复杂的核心。为平衡这两种需要，CPU生产厂商提出了将多个性能不同的处理器集成在用一个芯片中的思路，这就是非对称的多核处理器。

非对称多核处理器为从结构角度降低处理器功耗提供了思路[11]。不同的应用程序往往对处理器资源有不同的需求。拥有大量并行指令的程序适合运行在一个超标量的处理器上，因为超标量处理器能在一个时钟周期同时执行多条指令，但不包含并行指令的程序运行在超标量处理器上就无法发挥它的特点。相反，这样的程序更适合运行在一个单流水线的处理器上，这样的处理器在硬件上比超标量处理器简单的多，所消耗的电能也少得多。所以，在同一个芯片上集成多个计算能力、类型、功耗都不同的处理器，以适应不同类型应用程序的需要，与采用完全相同核心的处理器(对称多核处理器)相比较，可以显著节省处理器的功耗。

目前，各个CPU制造商推出的非对称多核处理器还都只使用两种不同性能的核心，例如，IBM Cell处理器、Intel Many Core处理器。但在同一芯片中集成多个不同性能、面向不同类型应用程序的处理器，必然是多核领域的一个趋势。

6 改进的RMT技术

多核处理器的出现为线程级并行技术的发展提供了广阔的空间。冗余多线程技术(Redundant MultiThreading，RMT)[8]正是借着这样的契机出现的一种应用于多核处理器的容错算法。其思想是，将一个程序复制为多份，并作为不同的线程在多条流水线上同时执行，通过一个判断逻辑对各个线程的结果进行比较、判断，选出正确的结果。这种重复利用硬件资源的技术可以防止处理器运行出错。但是，RMT技术存在显著的能耗问题，为了保证程序的正确性，处理器不得不承担多条流水线的能耗。

改进的RMT技术是针对RMT技术的功耗问题引入的。其思想是：将一个程序分成连续的程序块，一个主处理器按顺序运行各个程序块；两个或多个处理器作为检查器，验证主处理器运行的结果是否正确；在检查器上，采用各种降低功耗的技术(如动态电压调节)，从而降低整个程序运行的功耗。图5[9]展示了改进的RMT技术的工作机制：

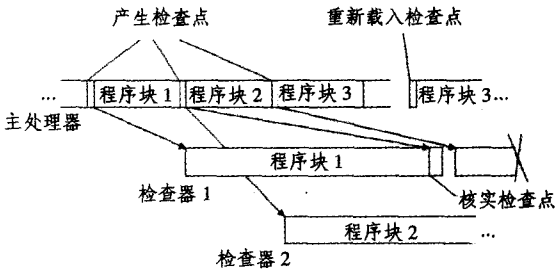

图5 改进的RMT技术

将一个程序分成包含一系列连续指令的程序块，在主处理器上按顺序执行。每个程序块执行完时，主处理器都产生一个检查点，检查点中包含该程序块每条指令执行的结果，包括数据和地址，还包含该程序块执行结束时各个寄存器的内容。检查点产生后，被存放到一个SRAM中，用于检查器判断主处理器执行的正确性和在发现错误时重新执行。主处理器执行程序的同时，将程序块分配到不同的检查器中执行。分配过程中，主处理器要将程序块的初始寄存器状态也提供给检查器。检查器将每条指令的执行结果同检查点中的结果相比较。执行结束时，还要将寄存器的状态同检查点比较。如果发现某条指令的结果与检查点中不同，检查器将通知主处理器，主处理器回滚到该条指令继续向下执行。

改进的RMT技术有很多优势。首先，由于不需要处理器在速度上的同步，检查器可以采用各种降低功耗的技术，比传统的RMT技术节省大量电能；而且，主处理器可以将程序执行的很多辅助数据放在检查点中，供检查器利用，例如分支预测的结果和跳转指令的目标地址。同时，cache的命中率也会显著提高，因为程序中用到的数据已经被主处理器取到L2 cache中。实验证明[9]，利用这些辅助数据，检查器的速度可以比以往提高平均35%。

它的缺点是为存放检查点，需要增加昂贵的SRAM；另外，一旦出现错误，无论发生在主处理器还是检查器，主处理器都必须回滚，这会影响程序执行的速度，降低吞吐率。如果频繁发生错误，由增加执行时间造成的能耗增加将会抵消检

查器上采用降低功耗技术而节省的电能。

总结和展望 本文就目前存在的降低处理器功耗的技术和方法进行了简单阐述，包括降低动态消耗和静态消耗的技术、采用非对称多核处理器结构降低功耗的方法，以及一种针对线程级并行的优化算法。

目前，各处理器厂商都在自己的产品上综合采用各种降低静态消耗和动态消耗的技术。但这些技术都需要为处理器增加额外的逻辑线路才能实现，这些线路本身也会消耗能量，还会增加芯片的面积。有的技术甚至需要操作系统的支持，而且对处理器的性能和速度或多或少会产生影响。所以，越来越多地从结构和算法角度考虑功耗的降低，而不是单纯采用各种电路级的降低功耗技术，必然是将来处理器功耗领域的发展趋势。

参 考 文 献

1 Kim N S, Austin T, Baauw D, et al. University of Michigan, Ann Arbor. Leakage current: Moore's law meets static power. Computer, 2003,36(12): 68～75

2 Henzler S, Georgakos G, Eireiner M, et al. Dynamic state-retention flip-flop for fine-grained power gating with small design and power overhead. Solid-State Circuits, IEEE Journal, July 2006, 41(7):1654～1661

3 Chen C, Liu Z Z, Ma T P. Analysis of enhanced hot-carrier effects in scaled flash memory devices. Electron Devices, IEEE Transactions on, July 1998, 45(7):1524～1530

4 Chandrakasan A, Bowhill W, Fox F. Design of High-performance Microprocessor Circuits. IEEE Press, 2001

5 Mukheijee A, Marek-Sadowska M. Clock and power gating with timing closure. Design & Test of Computers, IEEE, May-June 2003, 20(3): 32～39

6 Benini L, De Micheli G. Automatic synthesis of low power gated clock finite state machine. IEEE Trans Computer-Aided Design, June 1996, IS:630～643

7 Nowka K J, Carpenter G D, MacDonald E W, et al. A 32-bit PowerPC System-on-a-Chip With Support for Dynamic Voltage Scaling and Dynamic Frequency Scaling. Solid-State Circuits, IEEE Journal, 2002, 37(11):1441～1447

8 Mukherjee S M, Kontz S, Reinhardt. Detailed Design and Evaluation of Redundant Multithreading Alternatives. In: Proc. Int'l Symp Computer Architecture, IEEE CS Press, 2002. 99～100

9 Rashid M W, Tan E J, Huang M C, et al. Power-Efficient Error Tolerance in Chip Multiprocessors. Micro. IEEE, 2005, 25(6): 60～70

10 Pering T, Burd T, Brodersen R W. The Simulation and Evaluation of Dynamic Voltage Scaling Algorithms. In: Proc. 1998 Int't Symp on Low Power Electronics Design

11 Kumar R, Farkas K, Jouppi N P, et al. Processor Power Reduction via Single-ISA Heterogeneous Multi-core Architectures. Computer Architecture Letters, IEEE, 2003, 2(1): 2～2

12 Igarashi M, Usami K, Nogami K, et al. A low-power design method using multiple supply voltages. Low Power Electronics and Design. In: Proceedings, 1997 International Symposium, Aut. 1997. 36～41

(上接第 223 页)

本文算法由流密码加密包体数据及后续的变换处理两部分组成，算法的安全性主要由选择的流密码决定。流密码可根据加密速度、强度等具体要求灵活选择。变换处理主要是可逆整数 S 变换，它是 Harr 小波变换的整数变换形式，实现起来非常高效、方便。每个包的包体数据独立加密，加密密钥也由两部分组成，第一部分是应用流密码的密钥，第二部分是收集起来的 sign(V_h)，必须同时获得这两部分密钥，才能正确解密图像。由于混沌密码系统对初值和参数具有高度的敏感性，因此即使密钥只有非常微小的差别，也会在较少的迭代次数后就会产生两组轨道迥异、互不相关的混沌序列。图 3 给出了使用正确密钥和随机错误密钥解密所得到的结果。在密码体制中，密钥的存储、管理和分配是一个值得重视的问题，对于 JPEG2000 可分级码流，文[9]提供了一个较好的密钥管理方案。

(a) (b)

图 3 (a)使用正确密钥解密的结果；(b) 使用错误密钥解密的结果

由于本文算法仅对 JPEG2000 码流的每个包的包体数据独立进行加密，加密过程不改动码流的原有标记码，并且通过整数 S 变换处理保证了加密后的包体数据不会产生新的标记码，因此原始码流的结构得到保持，这使得：

1)加密后的码流仍然能够被标准解码器识别并解码，并且原始码流所具有的特性与功能也得到保持；

2)加密后的图像能够通过网络中的任意中间节点传输而无须解密，保证了端对端的安全性；当在信道传输过程中受到干扰产生误码时，仍保持和原码流一致的抗误码和容错能力；

3)加密包体数据后，包体的大小并没有发生改变，因此压缩率保持与原码流一致。

结束语 本文提出了一种不破坏码流结构的 JPEG2000 加密算法，通过变换处理使得加密后的包体数据不会产生新的标记码，加密后的码流仍能被标准解码器解码，但解读出来的是内容被掩蔽的图像。原码流的特性均被保留了下来，压缩率也没有发生改变。通过模拟实验，显示了良好的加密效果，表明利用该方法对 JPEG2000 静态图像的加密保护是安全有效的。

参 考 文 献

1 Ando K, Watanabe O, Kiya H. Partial-scrambling of still images based on JPEG2000[C]. In: International Conference on Information, Communications, and Signal Processing, 2F2.5, CD-ROM, Singapore, Oct. 2001

2 Ando K, Watanabe O, Kiya H. Partial-scrambling of Images Encoded by JPEG2000[C]. IEICE Trans, 2002, J85-D-II(2): 282～290

3 Wee S J, Apostolopoulos J G. Secure Scalable Streaming and Secure Transcoding with JPEG-2000[C]. IEEE Int Image Processing, Sept. 2003, 1: I-205～208

4 Kiya H, Imaizumi S, Watanabe O. Partial scrambling of JPEG2000 Images without Generating Marker Codes[C]. In: Proc. of IEEE International Conference on Image Processing(ICIP), Sept. 2003

5 Watanabe O, Nakazaki A, Kiya H. A Fast Image-Scramble Method Using Public-Key Encryption Allowing Backward Compatibility with JPEG2000[C]. In: Proc. of International Conference on Image Processing (ICIP), Singapore, Oct. 2004

6 Watanabe O, Nakazaki A, Kiya H. A Scalable Encryption Method allowing Backward Compatibility with JPEG2000 Images[C]. In: IEEE International Symposium on Circuits and Systems, May 2005, 6:6324～6327

7 Information Technology - JPEG 2000 Image Coding System, Part 1: Core Coding System, ISO/IEC 15444-1:2000 (ISO/IEC JTC/SC 29/WG 1 N1646R, March 2000)

8 张旭东，卢国栋，冯健. 图像编码基础和小波压缩技术——原理、算法和标准[M]. 北京：清华大学出版社，2004

9 Imaizumi S, Watanabe O, Fujiyoshi M, et al. Generalized hierarchical encryption of JPEG 2000 codestreams for access control [C]. In: IEEE International Conference on Image Processing, Sept. 2005, 2: II-1094～1097