

可重构分簇式分组密码处理架构

李校南¹ 王雪瑞² 戴紫彬¹ 纪祥君¹

¹(解放军信息工程大学 河南 郑州 450004)

²(河南工程学院 河南 郑州 451191)

摘 要 针对现有可重构分组密码系统资源利用率低的问题,在分析分组密码算法处理特征的基础上,提出基于 Crossbar 互连的可重构分簇式分组密码处理架构 RCCPA (Reconfigurable Clustered Cipher Processing Architecture),研究了 RCCPA 的互连网络、分簇式寄存器堆及配置方式。RCCPA 通过重构互连网络可将各处理簇动态地重构成 4 个 32 bit 簇、2 个 64 bit 簇和 1 个 128 bit 簇,并可将可重构处理单元 RCU (Reconfigurable Cipher Processing Unit) 组织成多级流水的处理路径,满足了分组密码处理灵活性的要求,提高了 RCU 的利用率。采用 RCCPA 实现 AES/DES/IDEA 的处理性能分别达到了 2 867.2 Mbps、1 442.6 Mbps、1 462.4 Mbps。

关键词 密码处理 可重构 分组密码 Crossbar 分簇式

中图分类号 TP309 文献标识码 A DOI:10.3969/j.issn.1000-386x.2014.01.085

RECONFIGURABLE CLUSTERED BLOCK CIPHER PROCESSING ARCHITECTURE

Li Xiaonan¹ Wang Xuerui² Dai Zibin¹ Ji Xiangjun¹

¹(PLA Information Engineering University, Zhengzhou 450004, Henan, China)

²(Henan Institute of Engineering, Zhengzhou 451191, Henan, China)

Abstract In light of the problem that existing reconfigurable block cipher system has low efficiency in resource utilisation, on the basis of analysing the processing characteristics of block cipher algorithm, we propose a reconfigurable clustered block cipher processing architecture (RCCPA) which is bases on Crossbar mutual-connection, study the mutual-connection network of RCCPA, the clustered registers file and its configuration mode. The RCCPA can dynamically reconfigure each processing cluster into four 32-bit clusters, two 64-bit clusters and one 128-bit cluster through the reconfiguration mutual-connection network. Besides, it can organise the reconfigurable processing RCU into a multi-pipeline processing path, which satisfies the flexibility demand of block cipher processing and improves the utilisation rate of RCU. The performance of implementing AES/DES/IEDA using RCCPA can reach as high as 2 867.2 Mbps, 1 442.6 Mbps and 1 462.4 Mbps.

Keywords Cipher processing Reconfigurable Block cipher Crossbar Clustered

0 引 言

随着可重构技术研究的深入,面向分组密码处理的可重构架构日益增多。基于 VLIW 结构的处理架构有:可重构分簇式分组密码处理器 RCBP^[1]、多 Cluster 结构的安全处理器 Soph-SEC^[2]、可重构分组密码芯片结构 COBRA^[3]等,基于 VLIW 结构的分组密码处理系统通过开发分组密码算法的指令级并行度,将可并行执行的指令组合成一条指令,在一个指令周期内完成,提高了分组密码算法的实现性能。但是上述结构每个时钟周期处理单元最多只能有一种运算逻辑工作,存在资源利用率低的问题。基于阵列结构的处理架构有:可重构密码处理结构 RC-PA^[4]、可重构层次互连密码处理结构 RHCA^[5]等,基于阵列结构的分组密码处理系统能够以较大的并行度和流水深度进行密码处理,但是阵列结构存在处理粒度小、互联资源多、布局布线复杂等问题,并且文献[4,5]提出的处理架构采用同构化设计,功能单元的利用率低下。

本文针对分组密码算法的处理特征,提取分组密码算法的

共性逻辑,立足提高可重构功能单元的利用率,开发密码算法实现的并行性,提出了基于 Crossbar 互连的可重构分簇式密码处理架构 RCCPA,完成了 RCCPA 的原型设计,并评估了分组密码算法在该结构上的映射及实现性能。

1 分组密码算法处理特征分析

分组密码大都基于相似的设计理论,如基于 Feistel 网结构或扩展 Feistel 网结构设计的 DES、FEAL、Lucifer、LOKI、GOST、DFC、MARS 及 RC6 等算法;基于 SP 网络结构设计的 CRYPTON、SAFER、AES 及 SERPENT 等;基于不同代数群的混合运算来设计的 IDEA、MMB 等。基于相同或相似设计理论的分组密码有相似的处理结构、操作类型较大交集^[5]。通过分析常见的分组密码算法,可以归纳出分组密码处理结构特点:

(1) 计算粒度,分组密码算法的分组长度一般为 64/128 位,分组密码算法运算过程中的处理粒度一般为 8~32 位,并以

收稿日期:2012-09-18。李校南,硕士生,主研领域:专用集成电路设计。王雪瑞,讲师。戴紫彬,教授。纪祥君,硕士生。

32 位的运算位宽较为常见,因此本文设计的可重构密码处理单元 RCU 的处理位宽为 32 bit。

(2) 并行处理,如图 1 所示,横向上分组密码算法大都是将数据分组拆分为字长数据,各个字并行处理。纵向上多个分组数据,在无反馈模式下,通过设置多个处理单元可以实现多个分组的流水操作;在反馈模式下,采用交替技术,也可以实现多个分组数据在多个处理单元上的流水操作。

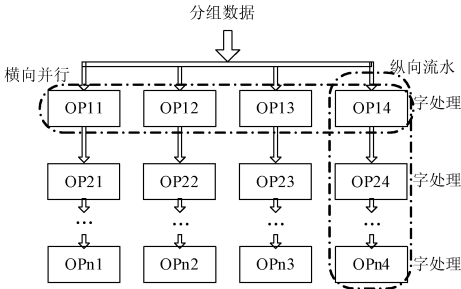


图 1 分组密码处理横向与纵向上的并行性

(3) 分支控制,分组密码算法的轮运算基本相同,算法各操作之间存在前后数据相关,但是分支较少、反馈较少,因此分组密码算法控制相对简单,适合流水执行。

(4) 操作类型,各分组密码算法的操作类型交集较大,基本上由 9 类基本操作完成:基本逻辑运算、模加/减运算、固定移位操作、变量移位操作、S 盒替代操作、置换操作、模乘运算、模乘逆运算、有限域 GF(2^n) 上乘法运算等。

通过对 DES、IDEA、AES 候选算法等 41 种公开的分组密码算法加解密结构进行分析研究,可以得出分组密码算法 9 类基本操作在各算法中的应用情况如图 2 所示。

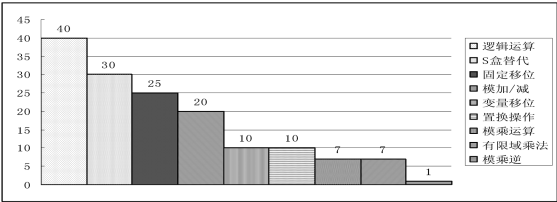


图 2 41 种流行分组密码算法的基本操作

从图 2 可以看出,除模乘逆之外,其它基本操作在 41 中分组密码算法中所占比例都超过 15% 以上。根据统计分析结果,运用可重构设计思想,共设计了 6 种 32 bit 位宽的可重构密码处理单元 RCU: S 盒替代单元、32 bit 移位单元、有限域 GF(2^n) 上的矩阵乘法单元、算术乘法单元、算术模加/减单元、逻辑运算单元等,为了对 SERPENT、CRYPTON 等算法中出现的 128 bit 置换及 IDEA 中涉及的 128 bit 长移位提供支持,专门设计了 2 个超长位宽 (128 bit) 的处理单元:128 bit 的置换单元和 128 bit 的移位单元。另外由同余定理和费马定理可知,模乘逆运算可以通过反复调用模乘操作得以实现,并且模乘逆运算应用较少,因此不再设计模乘逆运算单元。

2 可重构分簇式分组密码处理架构

分组密码算法适于分组(或分块数据)内并行、分组间并行或流水处理,并且具有分组(或分块数据)间数据交互少的特点,本文在分析分组密码算法特点、提取分组密码算法共性逻辑的基础上,提出了基于 Crossbar 互连的可重构分簇式密码处理架构 RCCPA,并重点研究互连网络、寄存器堆、配置方式等

问题。

2.1 总体架构设计

结合分组密码算法处理特点,本文提出的 RCCPA 架构如图 3 所示。架构采用分簇式设计,包含 4 个处理簇、配置单元、通用寄存器堆、子密钥寄存器堆、控制逻辑和 I/O 接口,每个处理簇包含有针对分组密码算法设计的 8 种可重构密码处理单元 RCU,对于超长处理位宽 (128 bit) 的可重构处理单元:比特置换、长移位单元将其输入、输出信号分为 4 组 32 比特接入到 4 个处理簇中。处理簇内的 RCU 通过基于 Crossbar 互连的 Level-1 总线进行数据交互,任一 RCU 的输出可以接到任一 RCU 的输入上,不同簇间的数据交互通过 Level-2 总线完成。RCCPA 可以根据密码处理的需要,灵活配置簇内、簇间的互连结构,在纵向和横向上组织各个 RCU,组成不同的处理路径,充分适应密码处理的并行及流水特性,完成密码运算。

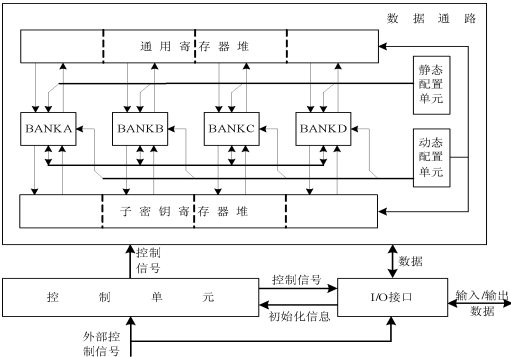


图 3 可重构分簇式密码处理架构

配置单元包括静态配置单元和动态配置单元两部分,其中静态配置主要完成各功能单元的功能配置,动态配置单元根据密码算法的处理流程动态重构互连网络,完成密码处理。通用寄存器用于存储密码处理过程中产生的输入/输出/临时数据,子密钥寄存器用于存储密码运算需要的子密钥数据、常数及 IV 向量。

在可重构分簇式密码处理架构 RCCPA 中,配置数据首先在控制单元的控制下分别存储于动态配置单元及静态配置单元中,控制单元根据静态配置单元中存储的配置信息完成可重构处理单元 RCU 的配置,完成静态配置后,RCCPA 接收外部输入的数据进行子密钥生成或密码处理运算,此时控制单元根据动态配置单元的内容动态配置互连网络,控制处理数据的处理序列及输入、输出,并实时地将状态信息写入到标志寄存器中。此外控制单元还可对无需参与运算的 RCU 进行旁路处理,以减小系统时延提高性能。

2.2 互连网络设计

可重构密码处理器的内部连接网络是各个基本密码运算模块之间进行数据传输的通路。其功能和特性对可重构密码处理器的灵活性、适应性、扩展性、性能和规模具有至关重要的影响[6]。常用的内部连接网络主要包括:全互连网络、单总线网络、多总线网络等,相对于其它两种互联方式,全互连网络具有最大的网络宽度,并且采用 Crossbar 实现的全互连网络可以动态重构,灵活性高。较大的网络宽度和较强的灵活性,可以提升分组密码处理架构的处理性能和适应性。因此本文选用基于 Crossbar 的互连网络实现 RCCPA 中各功能的连接。但是全互连网络规模较大,当处理单元增多时,其网络规模增长较快。分组密码算法的功能单元数量不多,且分组(或分块数据)间数据

信息交互较少,因此可以通过分簇、分级的方式设计互连网络,以减小互连网络的规模。本文基于以上分析设计了 Level-1、Level-2 两级互连结构,每个处理簇包含 1 个 Level-1 互连结构,用于簇内各个可重构处理单元 RCU 之间的互连。Level-2 互连结构用于簇间的数据交互。

如图 4 所示簇内采用 Level-1 的全 Crossbar 互连实现簇内 8 个功能单元间的全连接,Level-1 互连结构还将通用寄存器堆数据、输入寄存器数据接入到互连网络上,以实现上述数据到各 RCU 的连接。同时为了保证处理结果输出灵活性,Level-1 互连结构专门设置了数据输出端口,使处理结果可以灵活地写入到通用寄存器堆、子密钥寄存器堆以及输出寄存器堆。Level 互连结构的位宽设置与各 RCU 的处理位宽一致均为 32 bit。

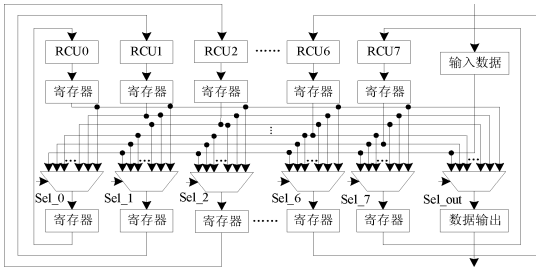


图 4 簇内的 Level-1 互连结构

为实现 4 个处理簇之间的数据交互,在 RCCPA 中设置了 Level-2 互连结构,在每个处理簇中设置了 6 个输入端口、6 个输出端口,每个端口的位宽为 32 bit,分别用于接收其它 3 个 BANK 的运算结果或将当前 BANK 的运算结果发送到其他 BANK,其互连结构如图 5 所示。

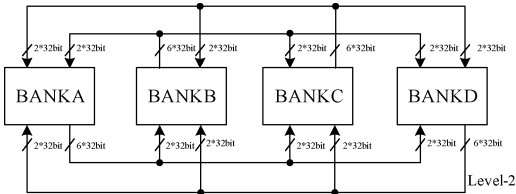


图 5 簇间通信结构

通过动态重构互连网络可以将各 BANK 中的 RCU 配置成处理分组密码运算的数据路径,图 6 给出了一种配置方式下形成的数据路径:数据输入 -> RCU6 -> RCU1 -> RCU0 -> RCU2 -> 结果输出。数据路径中多个 RCU 协同工作,形成多级流水线,可以同时处理多个密码分组,提高了 RCU 资源利用率。同时通过 Level-2 总线互连,还可以将数据路径动态地重构为 4 个 32 bit 簇、2 个 64 bit 簇和 1 个 128 bit 簇,满足了分组密码处理灵活性的要求。

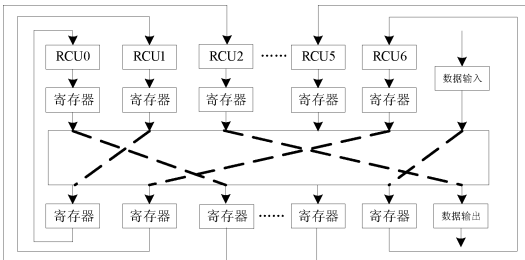


图 6 簇内 RCU 组成的数据路径

2.3 分簇式寄存器堆设计

分组密码处理过程中存储的数据大致可分为三类:S 盒查找表数据、子密钥数据、输入/输出/临时数据,S 盒查找表数据

存储在功能单元内部设置的存储器中,与寄存器结构无关。另外两类数据有着不同的用途、使用特点^[7]:子密钥一般数据量较多,占用较大的存储空间,但在加解密处理过程中保持不变,只有在主密钥变更时,才会由密钥扩展程序重新计算生成;输入、输出和计算过程中临时数据的存储容量需求不大,但其中某些数据需要频繁的改变。为此设计了两个寄存器堆:子密钥寄存器堆和通用寄存器堆,实现对两类不同数据的存储,寄存器堆采用分簇式设计,其整体结构如图 7 所示。

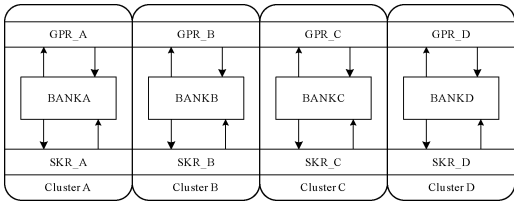


图 7 分簇式存储器结构

通用寄存器堆采用 4 个独立的寄存器堆实现:GPR_A、GPR_B、GPR_C、GPR_D,每个通用寄存器堆包括 1 个任意写端口和 1 个任意读端口,通用寄存器堆 GPR_A 只能由 BANKA 直接读写,相应的 GPR_B、GPR_C、GPR_D 只能由对应的 BANKB、BANKC、BANKD 直接读写。由于互连结构提供了簇间交互机制,当 BANK 需要使用其他 BANK 对应的寄存器数据时,可以通过 Level-2 互连总线进行读取。根据相同原理设计了子密钥寄存器堆,其读写机制与通用寄存器堆类似,只是面向的功能应用不同,存储空间不同。

RCCPA 设计的 4 个密钥寄存器堆的容量为:128 × 32,通用寄存器堆的容量为:64 × 32 bit。通用寄存器堆与密钥寄存器堆的整体结构如下图 8 所示。通用寄存器堆的输出直接接入到各 BANK 的互连网络上,每个 BANK 通过互连网络可直接对本 BANK 所对应的通用寄存器堆进行读写操作,系统可以通过 Level-2 总线间接读写其它 BANK 所对应的通用寄存器。子密钥寄存器堆的设计思想与通用寄存器堆类似,只是子密钥寄存器堆的输出直接接入 BANK 的功能单元上。

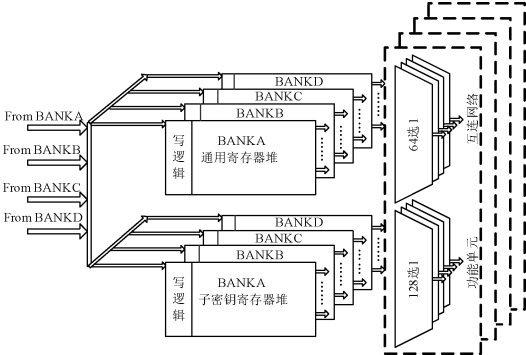


图 8 寄存器堆结构

2.4 配置方式研究与设计

采用静态配置与动态配置相结合的方式完成 RCCPA 中可重构密码处理单元 RCU 与互连网络的配置,RCU 的配置采用静态配置,互连网络的配置采用动态配置。RCCPA 中 RCU 所需要的配置信息存储于 RCU 的专用配置寄存器中,当需要执行某个配置时,控制单元通过静态配置的方式将配置信息写入到 RCU 相应的专用配置寄存器中。互连网络的配置信息存储于配置信息存储器中,在算法执行的每一个时钟周期,控制单元将配置信息动态译码输入到相应的互连网络的控制端,组织成不

同的数据通路。动态配置互连网络的方式有效减少了配置指令的长度,降低了译码的复杂性,同时保持了较高的编程深度和重构灵活性。

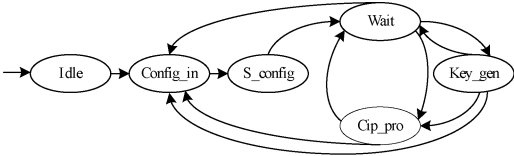


图9 控制单元的状态转换

RCCPA 在控制单元的控制下完成分组密码处理,控制单元通过状态机实现。RCCPA 架构的控制单元各状态之间的转换如图 9 所示,共包括 6 种状态:Idle、Config_in、S_config、Wait、Key_gen、Cip_pro。控制单元各状态的具体含义及转换条件如表 1 所示。

表 1 状态描述及触发操作

状态	状态描述及触发操作
Idle	空闲,上电或复位 Reset 有效,进入空闲态
Config_in	配置信息输入,当检测到 Addr = 3'b000、配置信息写入启动信号 Start 有效,进入该状态
S_config	静态配置,当检测到配置信息写入结束信号 Finsh 有效,进入该状态
Wait	等待,当静态配置完成即静态配置电路检测到静态配置完成指令或子密钥生成完成或密码处理完成,并且没有输入时,进入该状态
Key_gen	子密钥生成,检测到 Addr = 3'b001 且写使能有效,进入该状态
Cip_pro	密码处理,检测到 Addr = 3'b010、写使能有效且子密钥生成完成,则进入该状态

3 原型验证与性能分析

以分组长度和密钥长度都是 128 位、圈数为 10 的 AES 算法为例,说明分组密码算法在 RCCPA 上的映射。AES 由三部分组成:初始圈密钥加法,圈变换和末尾圈变换。初始圈密钥加法是将输入的明文与初始子密钥进行异或。算法中除了末尾圈变换省略列混合变换外,每圈变换包含字节代替变换、行移位变换、列混合变换和圈密钥加法,因此将 4 种可重构处理单元 RCU;S 盒替代单元、置换单元、有限域 GF(2ⁿ)上的矩阵乘法单元、逻辑运算单元组成数据路径。由于 RCU 与互连网络输出都含有一级寄存器,因此共可流水处理 8 个数据分组,AES 算法在 RCCPA 上的映射如图 10 所示。

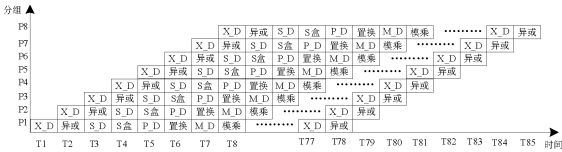


图10 AES 在 RCCPA 上的映射

为验证设计的正确性,使用 NC-Verilog 对可重构分簇式密码处理架构 RCCPA 进行了仿真测试。使用 Synopsys 公司的 Design Compiler for Solaris 工具,采用 0.13 μm CMOS 工艺标准单元库及相应负载模型和 RAM 硬核对 RCCPA 进行逻辑综合,综合结果如表 2 所示。

表 2 基于 ASIC 的 RCCPA 实现性能

约束(ns)	面积(um2)	等效门数	Slack	工作频率
4.2	8 749 072	145.82 万门	0.01	238 Mhz

经算法适配验证,RCCPA 可灵活适配 Feistel 网结构或扩展 Feistel 网结构、SP 网结构、代数群混合结构的常用算法。为了对比 RCCPA 的实现性能,选择不同结构、不同位宽的 AES、DES、IDEA 算法的实现性能,与其它可重构分组密码处理器进行了对比,性能对比结果如表 3 所示。

表 3 算法实现性能比较

单位:Mbps

算法	RCBCP	Crypto-nite	RCPA	RCCPA
AES	689.6	731	794	2 867.2
DES	400	128	460.8	1 442.6
IDEA	416.7	569	404.21	1 462.4

RCBCP^[1]是一款采用 VLIW 结构设计的具有 4 路并行的可重构分簇式密码处理器,Crypto-nite^[8]采用两路并行的 RISC 结构,每路 RISC 处理位宽为 64 bit,RCPA^[4]是基于阵列结构的可重构密码处理架构。通过适配多种分组密码算法及表 4 对比结果可以得出,RCCPA 结构可以灵活适配分组密码算法,并且对不同设计结构、不同处理位宽、不同操作位宽的分组密码算法均有较高的处理性能,与其它专用可重构密码处理结构相比处理性能提高了 2.5~11.3 倍。

4 结 语

本文在分析分组密码算法处理特征的基础上,立足于提高可重构处理单元 RCU 的利用率,设计了基于 Crossbar 互连的可重构分簇式密码处理架构 RCCPA,通过动态重构互连网络的方式,可将数据路径动态地重构成 4 个 32 bit 簇、2 个 64 bit 簇和 1 个 128 bit 簇,并可可将可重构处理单元 RCU 组织成多级流水的处理路径,满足了分组密码处理灵活性的要求。基于分簇式的处理架构,降低了互连网络、寄存器堆设计的复杂性。静态重构与动态重构相结合的配置方式,提高了分组密码适配的灵活性,降低了配置译码的复杂性。与其他可重构分组密码处理架构相比,RCCPA 具有更大的灵活性、更高的资源利用率和更强的处理性能。

参 考 文 献

[1] 孟涛,戴紫彬. 分组密码处理器的可重构分簇式架构[J]. 电子与信息学报,2009,32(2):453-456.

[2] 黄伟. 面向云计算的性能与功耗可配置安全终端技术研究[D]. 上海:复旦大学,2011.

[3] Adam J Elbirt. Reconfigurable Computing For Symmetric-Key Algorithms[D]. Massachusetts: Electrical and Computer Engineering Department University of Massachusetts Lowell,2002.

[4] 杨晓辉,戴紫彬,张永福. 可重构分组密码处理结构模型研究与设计[J]. 计算机研究与发展,2009,46(6):962-967.

[5] 姜晶菲. 可重构密码处理结构的研究与设计[D]. 长沙:国防科技大学,2004.

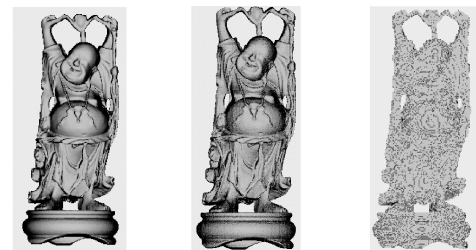
[6] 曲英杰. 可重构密码处理器内部连接网络的设计与分析[J]. 计算机工程与应用,2007,43(23):167-170.

表 3 添加顶点随机噪声时水印相关值

随机噪声强度	Happy Buddha	Dragon	Simple Happy Buddha	Simple Dragon
0.001	1.0	1.0	1.0	1.0
0.003	0.56	0.53	0.49	0.46
0.005	0.32	0.29	0.28	0.26

(3) 算法对模型顶点坐标值量化处理的实验结果

顶点坐标值量化处理采用低强度进行时,仍然可认为模型处于“内容保持”的范围内(如图 4(a)所示),但处理强度过高时,模型外观将会出现严重失真(如图 4(b)、(c)所示),应视为恶意攻击。顶点坐标量化处理时水印相关值结果如表 4 所示,可以看出本文算法嵌入的半脆弱水印对于低强度的顶点坐标量化处理表现并不敏感,而随着量化处理强度增加,水印相关值急剧下降。



(a) 精度 4 位 (b)精度 3 位 (c)精度 2 位

图 4 顶点坐标值量化对模型造成的外观失真

表 4 添加顶点随机噪声时水印相关值

顶点坐标浮点数精度	Happy Buddha	Dragon	Simple Happy Buddha	Simple Dragon
5	1.0	1.0	1.0	1.0
4	1.0	1.0	1.0	1.0
3	0.69	0.65	0.62	0.59
2	0.32	0.29	0.27	0.25

(4) 与其他三维网格模型半脆弱水印算法的比较

与本文算法进行比较的网格模型半脆弱水印算法为 Wu 的算法^[6]、Cho 的算法^[7]、Lin 的算法^[8]、Chou 的算法^[9]。当网格模型面临恶意攻击时,本文算法与这些半脆弱算法均具有较好的判别能力;但在容忍网格正常数据处理能力方面,本文算法具有一定的优势,可同时容忍网格模型的 RST 相似变换和低强度的顶点坐标值量化处理和顶点随机噪声,而其他算法大多只能容忍部分类型网格正常数据处理。具体比较结果如表 5 所示。

表 5 本文算法与其他三维网格模型半脆弱水印算法的比较

	RST 相似变换处理	顶点随机噪声	顶点坐标值量化
本文算法	可容忍	可容忍强度为 0.001 的噪声	可容忍浮点数精度由 6 位削减到 4 位
Wu 的算法 ^[6]	· 可容忍	不能容忍	不能容忍
Cho 的算法 ^[7]	可容忍	不能容忍	不能容忍
Lin 的算法 ^[8]	不能容忍	可容忍强度为 0.001 的噪声	可容忍浮点数精度由 6 位削减到 3 位
Chou 的算法 ^[9]	可容忍	不能容忍	不能容忍

5 结 语

半脆弱水印要求水印可容忍一些三维网格模型的正常数据处理,对于恶意攻击则表现敏感,与完全脆弱水印相比具有更广泛的适用范围。本文提出了一种基于内容级认证的三维网格模型半脆弱水印算法,将模型校准处理后进行二维参数化处理并嵌入半脆弱水印。实验结果表明,算法嵌入的水印可以良好地容忍三维网格模型的某些正常数据处理,如模型的平移、旋转、各向一致缩放、较低强度的顶点随机噪声等,但对于恶意攻击(例如较高强度的顶点随机噪声攻击)则表现敏感。不足之处为:本文算法比较适合用于复杂精细的三维网格模型(包含较多的顶点数目),对于简单的三维网格模型在进行球面坐标映射方阵处理时容易出现空洞区域,造成水印嵌入出错,在下一步工作中,将研究可适用于各种类型三维网格的半脆弱水印算法。

参 考 文 献

[1] Luo Ming, Bors A G. Surface-Preserving Robust Watermarking of 3-D Shapes[J]. IEEE Transactions on Image Processing, 2011, 20 (10) : 2813 - 2826.

[2] Zafeiriou S, Tefas A, Pitas I. Blind robust watermarking schemes for copyright protection of 3D mesh objects[J]. IEEE Transactions on Visualization and Computer Graphics, 2005, 11 (5) : 596 - 607.

[3] Cho J W, Prost R, Jung H Y. An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms [J]. IEEE Transactions on Signal Processing, 2007, 55 (1) : 142 - 155.

[4] Yeo B L, Yeung M. Watermarking 3D objects for verification [J]. IEEE Computer Graphics and Applications, 1999, 19 (1) : 36 - 45.

[5] Chou C M, Tseng D C. A public fragile watermarking scheme for 3D model authentication [J]. Computer-Aided Design, 2006, 38 (9) : 1154 - 1165.

[6] Wu H T, Cheung Y M. A high-capacity data hiding method for polygonal meshes [C]. Springer: LNCS, Volume, 2007, 4437 : 188 - 200.

[7] Cho W H, Lee M E, Lim H, et al. Watermarking technique for authentication of 3-D polygonal meshes [C] // Springer: LNCS, Volume, 2005, 3304 : 259 - 270.

[8] Lin H Y, Liao H Y M. Authentication of 3-D polygonal meshes [C] // Springer: LNCS, Volume, 2004, 2939 : 168 - 183.

[9] Chou Changmin, Tseng Dinchang. Affine-Transformation-Invariant Public Fragile Watermarking for 3D Model Authentication [J]. IEEE Computer Graphics and Applications, 2009, 29 (2) : 72 - 79.

[10] 崔晨阳. 三维模型检索中关键技术的研究 [D]. 浙江: 浙江大学, 2005.

[11] 孙树森. 三维模型数字水印技术及防重构技术研究 [D]. 浙江: 浙江大学, 2006.


(上接第 318 页)

[7] 戴紫彬. 面向分组密码处理的协处理器体系结构研究与设计实现 [D]. 解放军信息工程大学, 2007.

[8] Buchty R. CRYPTONITE: A programmable crypto processor architecture for high- bandwidth applications [D]. Munchen: Institut fur Informatik der Technischen Universitat Munchen, 2002.

作者: [李校南](#), [王雪瑞](#), [戴紫彬](#), [纪祥君](#), [Li Xiaonan](#), [Wang Xuerui](#), [Dai Zibin](#), [Ji Xiangjun](#)

作者单位: [李校南, 戴紫彬, 纪祥君, Li Xiaonan, Dai Zibin, Ji Xiangjun \(解放军信息工程大学 河南 郑州 450004\)](#), [王雪瑞, Wang Xuerui \(河南工程学院 河南 郑州451191\)](#)

刊名: [计算机应用与软件](#) 

英文刊名: [Computer Applications and Software](#)

年, 卷(期): 2014(1)

参考文献(8条)

1. [孟涛;戴紫彬 分组密码处理器的可重构分簇式架构](#) 2009(02)
2. [黄伟 面向云计算的性能与功耗可配置安全终端技术研究](#) 2011
3. [Adam J Elbirt Reconfigurable Computing For Symmetric-Key Algorithms](#) 2002
4. [杨晓辉;戴紫彬;张永福 可重构分组密码处理结构模型研究与设计](#) 2009(06)
5. [姜晶菲 可重构密码处理结构的研究与设计](#) 2004
6. [曲英杰 可重构密码处理器内部连接网络的设计与分析](#) 2007(23)
7. [戴紫彬 面向分组密码处理的协处理器体系结构研究与设计实现](#) 2007
8. [Buchtý R CRYPTONITE: A programmable crypto processor architecture for high-bandwidth applications](#) 2002

引用本文格式: [李校南. 王雪瑞, 戴紫彬. 纪祥君. Li Xiaonan. Wang Xuerui. Dai Zibin. Ji Xiangjun 可重构分簇式分组密码处理架构 \[期刊论文\]-计算机应用与软件](#) 2014(1)