Instituto Tecnológico de Costa Rica

Área Académica de Ingeniería en Computadores
(Computer Engineering Academic Area)

Programa de Licenciatura en Ingeniería en Computadores
(Licentiate Degree Program in Computer Engineering)

Curso: CE-4302 Arquitectura de Computadores II
(Course: CE-4302 Computer Architecture II)

Especificación Proyecto I
(Project II specification)

Profesor:
(Professor)

Ing. Jeferson González Gómez, M.Sc

Fecha de entrega : 19 de octubre, 2018
(Due Date: October 19th, 2018)

Proyecto II. Extensión SIMD a una arquitectura del set de instrucciones (ISA) para el procesamiento de imágenes

1. Objetivo

Mediante el desarrollo de este proyecto, el estudiante aplicará los conceptos de paralelismo a nivel de datos en la implementación de un computador con extensión SIMD al set de instrucciones de la arquitectura de un CPU para el manejo de operacionales vectoriales y escalares, en algoritmos de procesamiento digital de imágenes. La implementación de la arquitectura se desarrollará por medio de una plataforma de hardware FPGA DE1-SoC, de Altera.
Atributos relacionados: Análisis de problemas (AP), Diseño (DI).

2. Descripción general

El paralelismo a nivel de datos ha tenido históricamente un gran campo de aplicación. Desde los años 70's, el diseño e implementación de arquitecturas vectoriales ha tenido un desarrollo continuo, siendo los procesadores vectoriales la referencia para otros tipos de arquitecturas que utilizan el concepto de *Single-Instruction Multiple-Data* (SIMD) en una gran cantidad de aplicaciones. Con el avance de las tecnologías, los procesadores vectoriales han influenciado la extensión de arquitecturas escalares para la inclusión de operaciones vectoriales, de bajo nivel, soportadas por el hardware. Este procedimiento, conocido como extensión SIMD a la arquitectura del set de instrucciones, permite combinar la versatilidad y control de flujo de un procesador escalar convencional con el potencial paralelismo que se puede aprovechar al realizar operaciones vectoriales. El desarrollo de arquitecturas heterogéneas en las que se combinan diferentes tipos de paralelismo, entre ellos el paralelismo a nivel de datos, ha tenido un papel fundamental en los sistemas modernos. Los dispositivos móviles, por ejemplo, hacen uso de arquitecturas SIMD para favorecer el desempeño en ejecución de tareas relacionadas a multimedia, en las que el procesamiento paralelo es fundamental.

Para este proyecto se deberán aplicar los conceptos de arquitectura de computadores, vista como una combinación de elementos de software y hardware, en el diseño e implementación de la arquitectura y organización de un computador. Dicho computador, deberá poseer un procesador con arquitectura del set de instrucciones (ISA) extendida para la inclusión de operaciones vectoriales. La aplicación a ejecutar en el computador será del área del procesamiento digital de imágenes, en la que la cantidad de datos a procesar crea la necesidad de explotar el paralelismo a nivel de datos para lograr un mayor desempeño. El set de instrucciones base (original) deberá ser propuesto por cada grupo de trabajo,con base en algún criterio técnico. Pueden utilizarse versiones de sets comerciales como RISC-V, MIPS, ARM, o un set específico desarrollado a la medida para este proyecto (a aprobar por el profesor).

En el proyecto se desarrollará un acercamiento práctico la extensión de un set de instrucciones, diseño de hardware, teoría de compiladores y programación de sistemas computacionales en general.

3. Especificación

Para este proyecto se deberá diseñar e implementar a nivel de hardware una arquitectura del set de instrucciones extendida para el manejo de operaciones vectoriales en una aplicación de encriptación de imágenes en escala de grises. La arquitectura extendida incluirá un diseño de las instrucciones (o seudo instrucciones) vectoriales (número y tipo de instrucciones, formato de operandos, tamaño, encodificación, modos de direccionamiento, etc.), así como una implemetación del hardware del procesador como tal.

Una vez diseñado e integrado el sistema a nivel plataforma de hardware, se deberá diseñar una aplicación que aplique cuatro métodos de encriptación de imágenes que deberán realizarse a cada uno de los pixeles de la misma. En este punto, la extensión vectorial a la arquitectura favorecerá el desempeño del sistema al aplicar la tarea de procesamiento al menos a 4 pixeles simultáneamente, por medio de algún mecanismo de implementación paralela de operaciones vectoriales.

A continuación se describe a mayor detalle la especificación del proyecto:

ISA y extensión

Para el desarrollo del proyecto deberá plantearse como punto inicial la arquitectura del set de instrucciones (ISA) que utilizará como base para implementación del procesador, así como la programación sobre el mismo. El set de instrucciones deberá poseer la documentación adecuada sobre todos los elementos de la arquitectura. Será importante detallar cada una de las instrucciones en cuanto a funcionalidad, sintaxis, modos de direccionamiento, formato, tipo de datos, encodificación, etc. En este punto debe tenerse en cuenta además la cantidad y tipo de registros de propósito general, y la interfaz con memoria (esquema Von Neumann, Hardward). Cada decisión tomada en la extensión del set de instrucciones deberá ser justificada con base a la aplicación específica (que se detalla más adelante) y aspectos de eficiencia, tomando en cuenta recursos (costo, área, potencia, etc). Como primer producto del proyecto, deberá generarse un documento con la descripción del set extendido, así como un hoja de referencia rápida al set con instrucciones o seudo-instrucciones vectoriales y los aspectos más importantes del mismo.

En general, la extensión del set diseñada deberá contar al menos con los siguientes tipos de instrucciones **vectoriales**: operaciones aritméticas, operaciones lógicas, carga, almacenamiento, desplazamientos regulares en ambas direcciones y desplazamientos circulares en ambas direcciones.

El tipo de dato del set extendido será vector de números enteros de 8 bits (el signo, o no, quedará a criterio de cada grupo con la debida justificación del caso). El tamaño del vector deberá ser de al menos 4 bytes, es decir cada vector deberá tener al menos 4 datos de 8 bits cada uno.

Se deberán adicionar al menos 12 instrucciones o seudo-instrucciones al set.

Será crítico que el set extendido sea completamente compatible con el set original. La modificación del set no debe afectar la funcionalidad de programas compilados antes de la misma.

Organización del computador

Desde el punto de vista de organización, la implementación deberá contener todos los componentes principales del computador (memoria, cpu, entradas y salidas, etc). Adicionalmente para el caso de la visualización de las imágenes, el sistema debe contar con un controlador VGA que permite mostrar adecuadamente tanto la imagen original como la filtrada.

Como soporte a la aplicación principal deberá diseñarse un script o módulo de software que permita la conversión del programa en lenguaje de bajo nivel (ensamblador) a lenguaje máquina, para posteriormente ser almacenado en la memoria de instrucciones del computador. El script o herramienta deberá realizar la revisión de errores semánticos o sintácticos en el programa, antes de realizar la traducción a lenguaje máquina.

Aplicación

Desde el punto de vista de uso de la arquitectura se deberá diseñar una aplicación que a partir de una imagen en escala de grises (directamente pre-cargada en memoria) aplique cada uno de los algoritmos de encriptación de imágenes que se describirán adelante. Luego del procesamiento, deberá mostrar la imagen original, la imagen encriptada y la imagen desencriptada, en pantalla.

Los algoritmos de encriptación serán los siguientes:

- **XOR** con clave privada: Este tipo de encriptación es uno de los más utilizados como base de algoritmos criptográficos complejos, como AES, por ejemplo. Para este algoritmo, al color (en grises) de cada pixel (i,j) deberá aplicársele una operación XOR con un dato de 8 bits, denominado clave privada. Para desencriptar una imagen encriptada con este algoritmo, debe aplicarse el mismo proceso.
- **Desplazamiento simple**: En este algoritmo se deberá aplicar un desplazamiento de una cantidad definida de bits entre 1 y 7 hacia cualquier dirección al valor de cada pixel. Para desencriptar se deberá aplicar un desplazamiento simple en la dirección contraria con la misma cantidad de bits. Este algoritmo generará pérdidas en la información a la hora de desencriptar.
- **Desplazamiento circular**: Este algoritmo será similar al anterior, pero el desplazamiento será circular, lo que implica que los datos que serán desplazados no se perderán, sino que pasan del bit más significativo al menos significativo y viceversa. Para desencriptar se deberá aplicar el desplazamiento circular en la dirección contraria a la encriptación para la misma cantidad de bits desplazados.
- **Suma simple**: En este algoritmo, al color de cada pixel dentro de un vector deberá sumársele un valor determinado dentro de otro vector (clave). Así para un vector de 4 pixeles [30,60,1,1], el vector clave a sumar (para toda la imagen) podrá ser, por ejemplo,

[12, 5, 100, 10] y el resultado de color para este primer vector de pixeles debe ser entonces [42,65,101,11]. Deberán considerarse problemas de desbordamiento. Para desencriptar deberá restarse cada vector de pixeles en la imagen con respecto al mismo vector clave definido previamente.

La aplicación con los algoritmos anteriores deberá ser diseñada tanto escalar como vectorialmente.

Métricas

Se deberán obtener métricas para la comparación del desempeño en tiempo de ejecución para ambos casos, por medio de simulación.
Como métricas de la eficiencia de la implementación del computador, se deberán obtener valores de potencia estimada, frecuencia máxima de operación y uso de recursos (celdas lógicas y registros), tanto de la implementación de la arquitectura original, como la extendida. Estos valores se incluirán además en la sección de resultados del *paper.*

Notas adicionales

- El desarrollo de este proyecto se dará en grupos de 3 personas.
- Todo diseño deberá tener al menos 2 propuestas detalladas adecuadamente y comparadas según criterios ingenieriles.

4. Entregables

Como entregables en este proyecto se evaluará lo siguiente:

- Presentación funcional completa (65 %). Se evaluará según rúbrica correspondiente.
- Paper (máximo 4 páginas) 15 %
  - Resumen
  - Introducción
  - Sistema desarrollado
  - Resultados
  - Conclusiones
  - Referencias
- Documentación de diseño (20 %)
  - Documento de descripción de arquitectura del set de instrucciones (ISA) extendido. Deberá incluir la descripción completa del set (descripción de instrucciones, encodificación, tipo de operandos, registros, etc.), así como la hoja de referencia rápida del mismo.(10 %)

- Metodología de diseño de sistema: Deberá detallar la metodología de diseño utilizada (explícitamente) en el proyecto que involucre el análisis del problema (con extracción de requerimientos), investigación respectiva, propuestas de diseño, comparación y evaluación de propuestas y verificación de requemientos. (10 %)