UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Leandro Perin de Oliveira

USO DE COMPUTAÇÃO PARALELA PARA ACELERAR A CRIPTO-COMPRESSÃO DE DADOS

Florianópolis
2017

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1. INTRODUÇÃO

Serviços como o YouTube, Instagram, Facebook, dentre outros, possuem uma enorme quantidade de dados armazenados, incluindo texto, imagens e vídeos. Com o aumento no uso de serviços como esses, maior tráfego de dados através da rede e necessidade de armazenamento cada vez maiores, são requeridos métodos mais eficientes para compressão de imagens e vídeos, com alta qualidade de reconstrução e redução na quantidade de armazenamento necessária para os dados.

A disponibilidade de um algoritmo de compressão de dados mais eficiente, que consiga reduzir mais o tamanho dos arquivos, comprimir de forma rápida, e ainda sim poder criptografar os dados é algo que melhoraria bastante o uso de serviços com alto tráfego de informações.

Tal algoritmo tornaria os serviços em nuvem mais populares, afinal deixaria os mesmos mais rápidos e seguros, encorajando o desenvolvimento de cada vez mais aplicativos que fazem uso de muitos dados.

1.1 JUSTIFICATIVA

A falta de um algoritmo mais eficiente para compressão e criptografia de dados multimídia tornam serviços na nuvem mais lentos, inseguros, com maior necessidade de armazenamento e maior uso da rede, afinal precisam armazenar e transmitir dados maiores e, muitas vezes, não cifrados, o que aumenta riscos de segurança.

Este trabalho poderá, também, ser integrado facilmente em projetos futuros que tenham restrições de infraestrutura, necessidade de maior velocidade de processamento ou maior segurança das informações, por exemplo.

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Tornar mais rápido e eficiente o algoritmo de cripto-compressão de dados desenvolvido num projeto da Universidade de Sheffield, no Reino Unido. Serão utilizadas técnicas de computação paralela e concorrente para acelerar a execução do algoritmo.

1.2.2 OBJETIVOS ESPECÍFICOS

- Produzir um código sequencial limpo e organizado do algoritmo;
- Paralelizar o código, fazendo o mesmo executar em vários núcleos da CPU;
- Estudar a possibilidade de paralelizar mais o código através do uso de GPUs;
- Desenvolver a monografia do trabalho;

1.3 CRONOGRAMA

	Atividades	Concluído	Início	Término
1	Produção do código sequencial limpo e organizado do algoritmo	Sim	01/08/2017	01/10/2017
2	Paralelização do código para execução em vários núcleos da CPU	Não	01/02/2018	01/03/2018
3	Estudar (e desenvolver) a execução do código em GPUs	Não	01/03/2018	01/04/2018
4	Monografia do trabalho	Não	01/04/2018	01/05/2018

1.4 LIMITAÇÕES

1.5 METODOLOGIA

A metodologia de pesquisa baseia-se em encontrar as melhores técnicas de computação paralela e concorrente, que possam auxiliar no desenvolvimento do trabalho proposto.

Tais técnicas serão estudadas, adaptadas para o projeto, implementadas e testadas para se escolher uma ou mais técnicas que se mostrem adequadas para o desenvolvimento do trabalho proposto.

1.6 ORGANIZAÇÃO DOS CAPÍTULOS

- Introdução: Será apresentado o problema, a importância de sua resolução e as metas do trabalho proposto;
- Fundamentação Teórica: Apresentação e explicação dos conceitos julgados necessários para o completo entendimento do trabalho;
- Desenvolvimento: Serão detalhadas as técnicas, estudos e testes feitos para se encontrar a melhor solução;
- Conclusão: Principais observações a serem feitas a respeito do trabalho desenvolvido, juntamente com os resultados alcançados. Também serão descritas possíveis melhorias e usos deste trabalho em projetos futuros;