USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

Nama : **Mohammad Zarkasi**
NRP : **5109 100 155**
Dosen Wali : **Waskitho Wibisono, S.Kom., M.Eng., PhD**

2. JUDUL TUGAS AKHIR

Implementasi Komputasi Paralel untuk Enkripsi Citra Berbasis AES Menggunakan Java Parallel Programming Framework

3. LATAR BELAKANG

Merahasiakan pesan sudah dilakukan sejak dulu saat elektronika belum ditemukan. Ada yang menggunakan simbol-simbol yang hanya bisa dimengerti oleh dua pihak yang berkomunikasi. Ada yang mengacak huruf-huruf dalam pesan menggunakan rumus matematika sederhana. Namun keamanan metode awal enkripsi ini sangat lemah. Metode ini dapat dipecahkan dengan metode-metode sederhana, seperti metode statistika[4].

Dalam beberapa tahun terakhir, tercatat pertumbuhan transmisi data digital yang sangat tinggi yang memanfaatkan adanya teknologi internet. Dalam kebanyakan kasus, kanal transmisi tidak cukup aman untuk menghindari akses ilegal oleh orang-orang yang tidak berhak. Oleh karena itu, keamanan dan kerahasiaan telah menjadi perhatian utama[6].

Gambar merupakan salah satu berkas yang banyak ditransmisikan melalui jaringan internet. Dalam beberapa kasus, misalkan ada seorang atau instansi yang akan memberikan gambar kepada orang lain melalui layanan internet. Namun, gambar yang akan dikirim merupakan gambar rahasia yang tidak boleh diketahui oleh orang lain kecuali si penerima. Namun ada kemungkinan ada orang yang bisa mengetahui bahwa ada pengiriman gambar rahasia dari pengirim ke penerima. Bisa saja gambar rahasia

tersebut merupakan desain prototipe suatu produk milik perusahaan terkenal. Apabila gambar rahasia itu bocor, ada kemungkinan perusahaan pesaing mengumumkan klaim terlebih dahulu atas desain produk dari gambar rahasia yang telah bocor.

Untuk mengatasi transmisi yang tidak aman, diterapkan enkripsi terhadap gambar digital. Enkripsi merupakan proses mengubah informasi dengan menggunakan suatu algoritma untuk membuat informasi tersebut tidak dapat dibaca oleh siapapun, kecuali orang-orang yang memiliki *key*[4].

Salah satu algoritma enkripsi yang cukup luas diterapkan yaitu AES (*Advanced Encryption Standard*) yang ditemukan oleh US National Institute of Standards and Technology (NIST) pada tahun 2002. AES merupakan jenis enkripsi blok dan terdapat beberapa ronde dalam proses enkripsinya. Dibandingkan dengan pendahulunya, yaitu DES, AES mampu berjalan lebih dan cepat efektif baik dari segi mesin maupun algoritma.

Namun, seiring dengan meningkatnya transaksi data digital, maka dibutuhkan cara yang lebih cepat untuk menjalankan algoritma enkripsi. Menerapkan komputasi secara paralel menjadi salah satu solusi untuk mempercepat enkripsi. Ada dua macam komputasi paralel, yaitu paralelisme data dan paralelisme kontrol[3].

Paralelisme data yaitu setiap node mengerjakan satu algoritma utuh namun data yang diolah merupakan bagian dari data yang utuh. Sedangkan paralelisme kontrol yaitu setiap node mengerjakan bagian algoritma tertentu dari suatu algoritma utuh namun data yang diolah adalah sama.

4. RUMUSAN MASALAH

Rumusan masalah yang diangkat dalam Tugas Akhir ini dapat dipaparkan sebagai berikut:

1. Bagaimana algoritma AES dapat digunakan untuk mengenkripsi gambar digital.
2. Bagaimana menerapkan komputasi paralel terhadap algoritma AES.
3. Bagaimana cara membagi data untuk diproses di tiap node.
4. Bagaimana menggabungkan hasil proses dari tiap-tiap node.

5. BATASAN MASALAH

Permasalahan yang dibahas dalam Tugas Akhir ini memiliki beberapa batasan, diantaranya sebagai berikut:

1. Sistem mampu melakukan enkripsi pada berkas gambar yang umum seperti JPG, JPG, BMP, dan PNG.
2. Sistem dapat dijalankan secara paralel di dua komputer berbeda.
3. Sistem dapat berjalan di sistem operasi Windows dan Linux.
4. Sistem tidak melakukan enkripsi pada berkas selain berkas gambar.
5. Output sistem adalah berkas gambar terenkripsi dengan ekstensi sama dengan yang diinputkan.

6. TUJUAN DAN MANFAAT TUGAS AKHIR

Tugas akhir ini bertujuan untuk :

1. Merancang dan membangun algoritma AES yang dapat digunakan untuk mengenkripsi gambar.
2. Merancang dan membangun sistem komputasi paralel yang menerapkan algoritma AES.
3. Merancang dan membangun sistem yang dapat membagi data untuk dienkripsi di beberapa node.
4. Merancang dan membangun sistem yang dapat mengolah hasil pengolahan enkripsi data di tiap-tiap node

Manfaat yang diharapkan dari tugas akhir ini adalah adanya suatu sistem enkripsi gambar yang dapat dijalankan secara paralel untuk mempercepat waktu proses enkripsi.

7. DASAR TEORI

7.1. Enkripsi

Enkripsi adalah proses tranformasi informasi (*plain text*) menggunakan suatu algoritma untuk membuatnya tidak terbaca oleh siapapun kecuali orang-orang yang memiliki pengetahuan khusus, biasanya disebut *key*. Hasil dari proses enkrispi adalah informasi yang telah terenkripsi yang biasa disebut dengan

ciphertext. Proses sebaliknya, yaitu proses membuat *ciphertext* dapat terbaca kembali menjadi *plaintext* disebut dengan dekripsi[4].

Enkripsi telah lama digunakan dalam bidang pemerintahan dan militer untuk mengamankan komunikasi rahasia yang dilakukan. Namun sekarang hal ini menjadi umum dilakukan dalam bidang sipil. Sebagai contoh hal yang sering kita hadapi adalah keamanan transaksi dalam internet. Banyak situs-situs yang ingin mengamankan informasi yang mereka kirimkan kepada klien menggunakan enkripsi. Karena sensitifnya informasi yang dikirim, enkripsi mutlak diperlukan. Hal ini untuk menghindari orang-orang yang "menguping" transaksi klien dengan server. Jika dalam transaksi tersebut, terdapat informasi-informasi penting, seperti informasi rekening bank, kartu kredit, dan lain sejenisnya, maka dengan mudah orang yang menguping dapat mengetahuinya jika dalam transaksi tersebut tidak digunakan enkripsi.

7.2. AES

Advanced Encryption Standard (AES) adalah sebuah ketentuan yang dibuat oleh *National Institute of Standards and Technology* (NIST), Amerika Serikat pada tahun 2002. Pada awalnya algoritma ini disebut Rijndael, diambil dari dua nama orang Belgia yang membangun algoritma AES, Joan Daemen dan Vincent Rijmen, yang diajukan ke proses seleksi AES[4].

AES menggantikan *Data Encryption Standard* (DES) yang dipublikasikan pada tahun 1977. Algoritma yang dijelaskan dalam AES adalah algoritma *symmetric-key*, yang artinya *key* yang sama digunakan untuk proses enkripsi dan dekripsi data. AES standar merupakan sebuah varian dari Rijndael yang ukuran bloknya dibatasi sebesar 128[4].

7.3. Komputasi Paralel

Komputasi paralel adalah suatu bentuk komputasi yang banyak perhitungannya dilakukan secara simultan, yang berprinsip pada masalah besar sering dapat dibagi menjadi yang lebih kecil, yang kemudian diselesaikan secara bersamaan. Ada berbagai macam komputasi paralel: *bit-level*, *instruction-level*, *data parallelism*

dan *task parallelism*. Paralelisme telah digunakan bertahun-tahun, terutama dalam komputasi yang membutuhkan kinerja tinggi. Perhatian akhir-akhir ini tertuju pada penskalaan frekuensi karena dibatasi kendala fisik[2].

Komputer paralel secara kasar dapat diklasifikasikan dalam beberapa level berdasarkan dukungan hardware terhadap paralelisme, komputer *multi-core* dan *multi-processor* yang memiliki elemen pemrosesan ganda dalam mesin tunggal. Arsitektur komputer paralel tertentu kadang digunakan bersama prosesor tradisional untuk mempercepat tugas-tugas tertentu.

Program komputer paralel lebih sulit ditulis daripada yang berurutan, karena *concurrency* memunculkan beberapa kelas baru yang berpotensial bug pada software, yang mana *race condition* adalah masalah yang utama. Komunikasi dan sinkronisasi antara *subtask* yang berbeda biasanya merupakan hambatan terbesar untuk mendapatkan kinerja program paralel yang baik.

7.4. JPPF

Dalam desain awalnya, JPPF merupakan *framework* pemrosesan paralel yang terdistribusi yang berdasarkan arsitektur *master/slave*[1]. Grid JPPF terbuat dari 3 macam komponen yang saling berkomunikasi: klien yang mengirimkan *work* ke grid, node yang menjalankan *work*, dan server yang menerima *work* dari klien dan mendistribusikannya ke *node* secara paralel. Poin penting dari JPPF adalah setiap *node* hanya bisa terjalin dengan satu server saja pada waktu tertentu. Tetapi tidak harus selalu terhubung ke server yang sama. Misalnya, jika koneksi ke server rusak, beberapa mekanisme *failover* memungkinkan node untuk terhubung ke server lain.

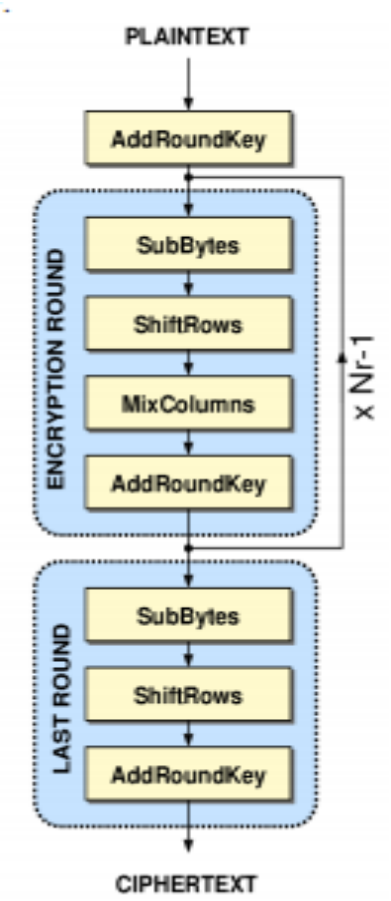
8. RINGKASAN TUGAS AKHIR

Pada tugas akhir ini penulis mengusulkan untuk merancang dan membuat sistem yang dapat mengenkripsi gambar digital yang dijalankan secara paralel. Sistem dibuat di atas framework komputasi paralel, yaitu JPPF. *Java Parallel Programming Framework*

(JPPF) adalah framework yang dibangun di atas bahasa pemrograman Java dan dapat berjalan di atas sistem operasi apapun yang mendukung Java.

Sistem yang dibangun adalah sistem untuk mengenkripsi gambar digital dengan berdasarkan algoritma AES. Sedangkan bagian yang dikerjakan secara paralel adalah data yang diolah. Tiap *node* mengerjakan satu bagian dari data utuh dan mengirimkan hasilnya ke *server* untuk diolah dengan hasil dari *node* lainnya.

Secara umum algoritma AES digambarkan sebagai berikut:



Gambar 1. Algoritma AES

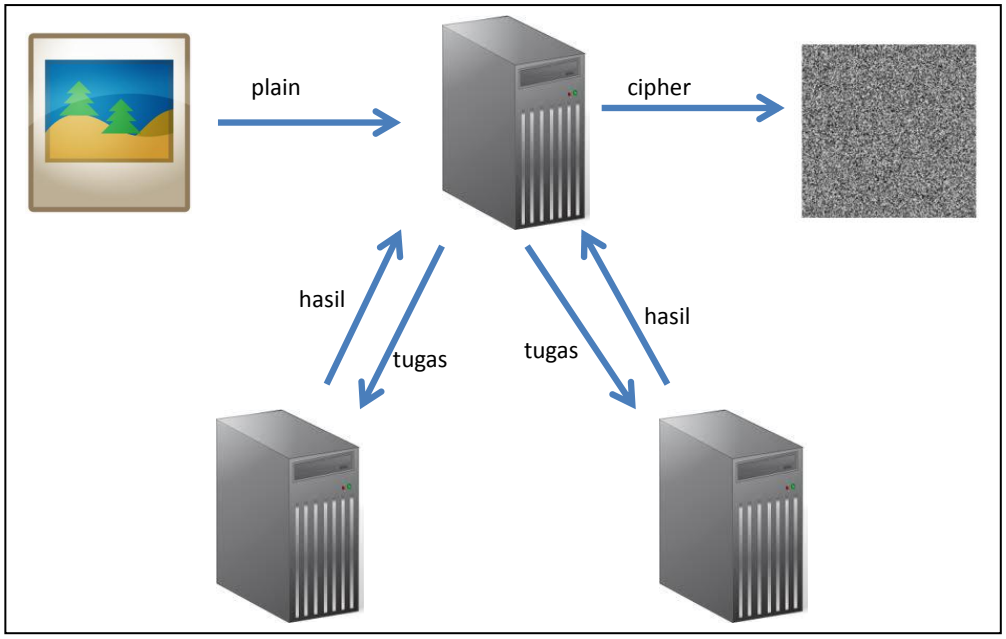
Ada 4 inti operasi pada algoritma AES, yaitu sebagai berikut:

1. SubBytes : operasi substitusi data dengan Sbox
2. ShiftRows : operasi transposisi data
3. MixColumn : operasi perkalian matrix data
4. AddRoundKey : operasi XOR data dengan *key*

Secara garis besar sistem yang dibangun memiliki fitur sebagai berikut:

1. Mampu menerima inputan berupa gambar yang umum, seperti JPG, JPEG, BMP, dan PNG
2. Mampu mengenkripsi gambar yang diupload dan menghasilkan cipher gambar.
3. Mampu menjalankan aplikasi secara paralel pada beberapa komputer secara bersamaan.

Analisis dan Perancangan



Gambar 2. Arsitektur Sistem Komputasi Paralel.

Dari Gambar 2 dapat dijelaskan sebagai berikut:

1. Citra plain diupload ke server
2. Server membagi pekerjaan kepada node-node
3. Hasil pekerjaan node dikirim kembali ke server
4. Server memberikan hasil enkripsi dalam bentuk citra yang sudah terenkripsi

9. METODOLOGI

Metodologi yang akan dilakukan dalam Tugas Akhir ini memiliki beberapa tahapan, diantaranya sebagai berikut:

1. Penyusunan Proposal Tugas Akhir

   Tahap awal untuk memulai pengerjaan Tugas Akhir adalah penyusunan Proposal Tugas Akhir. Pada proposal ini, penulis mengajukan gagasan perancangan dan pengembangan sistem enkripsi gambar yang dilakukan secara paralel dengan bantuan JPPF yang dibangun di atas bahasa Java.

2. Studi Literatur

   Pada tahapan ini akan dilakukan studi literatur mengenai cara yang digunakan untuk membuat sistem.

3. Implementasi

   Implementasi merupakan tahap pembangunan sistem enkripsi gambar. Implementasi menggunakan bantuan framework JPPF untuk membangun aplikasi yang dapat berjalan secara paralel.

4. Pengujian dan Evaluasi

   Pada tahap ini dilakukan uji coba terhadap sistem yang telah dibuat, dengan cara menilai apakah sistem sudah memadai dan sudah sesuai kebutuhan yang telah diidentifikasi sebelumnya.

5. Penyusunan Buku Tugas Akhir

   Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari implementasi perancangan dan pembuatan sistem yang telah dibuat. Secara garis besar, buku laporan tugas akhir ini terdiri atas beberapa bagian yaitu:

   1. Pendahuluan

      1.1 Latar Belakang

      1.2 Permasalahan

      1.3 Batasan Tugas Akhir

      1.4 Tujuan

      1.5 Metodologi

      1.6 Sistematika Penulisan

2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

10. JADWAL KEGIATAN TUGAS AKHIR

Tugas akhir ini diharapkan bisa dikerjakan menurut jadwal sebagai berikut:

No.	Kegiatan	2012				2013
		September	Oktober	November	Desember	Januari
1.	Penyusunan Proposal Tugas Akhir					
2.	Studi Literatur					
3.	Implementasi					
4.	Pengujian dan Evaluasi					
5.	Penyusunan Buku Tugas Akhir					

11. DAFTAR PUSTAKA

[1] *JPPF About* (http://www.jppf.org/about.php, diakses pada tanggal 3 Oktober 2012)

[2] Pacheco, P. 2011. *An Introduction to Parallel Programming.* Massachusetts: Morgan Kaufmann Publishers.

[3] Pachori, V., Ansari, G., & Chaudhary, N. 2012. Improved Performance of Advanced Encryption Standar using Parallel Computing. *International Journal of Engineering Reserach and Application*, 967-972.

[4] Stallings, W. 2011. *Cryptography and Network Security.* Prentice Hall.

[5] Zeghid, M., Machout, M., Baganne, A., & Tourki, R. 2007. A Modified AES Based Algorithm for Image Encryption. *International Journal of Computer Science and Engineering*, 70-75.

[6] Zhou, Q., Wong, K.-w., Liao, X., Xiang, T., & Hu, Y. 2007. Parallel image encryption algorithm based on discretized chaotic map. *ScienceDirect*, 1081-1092.