

**IMPLEMENTASI MODIFIKASI KUNCI
KRIPTOGRAFI RC6 YANG DIFUNGSIKAN
DENGAN BLUM BLUM SHUB PADA DIGITAL
IMAGE**

SKRIPSI

Disusun Oleh:

JAUHAR SAFRAINI

13.04.111.000.11



**PROGRAM STUDI INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS TRUNOJOYO MADURA
BANGKALAN
2019**

(Halaman ini sengaja dikosongkan)

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini informasi khususnya digital image telah menjadi aset yang sangat berharga baik suatu organisasi, perusahaan, pemerintah maupun pribadi. Hal ini karena keamanan dan kerahasiaan dari sebuah informasi sangat penting untuk dilindungi dari manipulasi informasi, pencurian informasi, serta dari serangan terhadap informasi yang secara langsung ataupun tidak langsung yang akan mempengaruhi kinerja. Informasi-informasi tersebut tentunya akan banyak diminati dari berbagai pihak yang juga memiliki kepentingan didalamnya. Terlebih lagi dengan perkembangan teknologi informasi yang sangat cepat ini, yang memberikan suatu kemudahan bagi kita untuk melakukan komunikasi dan pertukaran informasi melalui internet. Hal ini dapat meningkatkan sebuah tindakan dari kejahatan komputer yang dapat dilakukan dengan melalui teknologi contohnya seperti penyadapan, pencurian ataupun pertukaran data atau informasi.

Akhir-akhir ini, semakin banyak yang muncul sebagai software untuk mengedit dan memodifikasi image digital dengan mudah, bahkan kalangan awampun bisa menggunakannya. Hasil modifikasi mereka pun tidak sedikit yang negatif, baik untuk membuat fitnah, penggambaran seseorang ataupun sekelompok orang dari berbagai maksud lainnya.

Hal ini ternyata mengganggu para pemilik data dan juga pihak yang ingin berkomunikasi dalam bertukar informasi baik kepentingan pribadi maupun kelompok. Sehingga dapat dikatakan bahwa perlindungan suatu data atau informasi menjadi kebutuhan yang sangat penting untuk saat ini. Untuk itu diperlukan usaha pengamanan data supaya keaslian dan kerahasiannya bisa terjaga.

Usaha perlindungan data khususnya image dapat dilakukan dengan berbagai macam cara, salah satunya yaitu dengan cara mengaplikasikan bidang kriptografi. Kriptografi bisa dilakukan dengan mengenkripsi data image tersebut kedalam bentuk data lain yang tidak bisa dikenali (*ciphertext*). Untuk mengembalikan *ciphertext* menjadi seperti data semula (*plaintext*), dapat dilakukan dengan mendekripsi *ciphertext* yakni dengan menggunakan algoritma kebalikan atau invers pada *ciphertext* tersebut.

Data image pada umumnya memiliki ukuran yang relatif besar dibandingkan dengan teks, maka proses enkripsi menggunakan algoritma yang tidak sesuai akan memerlukan waktu yang cukup lama. Karena dikenal dengan kecepatan pemrosesan dan keamanannya maka peneliti menggunakan algoritma RC6 untuk penyandian pada image digital. Pada proses penyandian algoritma RC6 beroperasi byte ke byte sehingga menghasilkan suatu rangkaian byte yang dapat di implementasikan pada image digital menggunakan nilai pixel untuk proses penyandiannya.

Sedangkan keamanan yang dihasilkan dari penyandian image digital diperoleh dari kunci yang dilakukan dengan menggunakan algoritma RC6 yang dapat menghasilkan suatu aliran kunci acak dan tidak adanya perulangan kunci sehingga menjadikan keamanan informasi pada image digital dapat terjaga.

Algoritma RC6 menawarkan kesederhanaan dan fleksibilitas yang tinggi sehingga keamanan dari algoritma RC6 lebih baik dari rijndael. Kesederhanaan dari algoritma dapat dilihat dari operasi matematika dasar yang terdapat pada algoritma RC6 ini seperti penjumlahan, pengurangan, dan XOR. Sedangkan fleksibilitas algoritma ini dapat dilihat dari 3 parameter, ketiga parameter tersebut yaitu adalah panjang blok yang diolah atau ukuran register W dalam bit, banyak iterasi r , dan panjang kunci b sehingga image digital dapat diamankan lebih baik atas adanya variasi parameter yang ditawarkan. Algoritma yang dibahas dalam skripsi ini yaitu algoritma Rivest Code 6 (RC6) yang juga difungsikan dengan modifikasi kunci Blum Blum Shub. [1].

Salah satu modifikasi kunci pada kriptografi yang dapat dilakukan adalah dengan menambahkan proses matematis saat membangkitkan bilangan acak yang akan digunakan sebagai kunci enkripsi dan dekripsi, Blum Blum Shub (BBS) merupakan algoritma CSPRNG (*cryptographically secure pseudo random number generator*), yang dapat digunakan untuk membangkitkan deretan bilangan acak yang aman digunakan pada proses enkripsi. Diusulkan tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub.

1.2 Rumusan Masalah

Dari latar belakang masalah di atas permasalahan yang dikaji yaitu:

1. Berapa lama waktu yang diperlukan untuk menguji proses enkripsi dan dekripsi antara algoritma RC6 biasa dengan RC6 modifikasi yang difungsikan dengan Blum Blum Shub pada digital image?
2. Seberapa aman hasil pengujian *Avalanche Effect* antara algoritma RC6 biasa dengan RC6 modifikasi yang difungsikan dengan Blum Blum Shub pada digital image?
3. Seberapa efektif hasil pengujian PSNR antara algoritma RC6 biasa dengan RC6 modifikasi yang difungsikan dengan Blum Blum Shub pada digital image?

1.3 Tujuan dan Manfaat

Adapun Tujuan dan manfaat yang dapat diambil dari permasalahan diatas antara lain:

1.3.1 Tujuan

Tujuan dari penelitian ini yaitu sebagai berikut:

1. Untuk mengetahui lama waktu yang diperlukan untuk menguji proses enkripsi dan dekripsi antara algoritma RC6 biasa dan RC6 modifikasi yang difungsikan dengan Blum Blum Shub.
2. Untuk mengetahui seberapa aman hasil pengujian antara algoritma RC6 biasa dan RC6 modifikasi yang difungsikan dengan Blum Blum Shub.
3. Untuk mengetahui efektif hasil pengujian PSNR antara algoritma RC6 biasa dan RC6 modifikasi yang difungsikan dengan Blum Blum Shub.

1.3.2 Manfaat

Penelitian ini diharapkan untuk mengetahui performa kunci RC6 biasa dan kunci RC6 modifikasi yang menggunakan fungsi Blum Blum Shub

1.3.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah:

1. Image yang digunakan berformat JPG,
2. Implementasi algoritma RC6 pada image digital *grayscale* dan RGB.
3. Ukuran image yang diuji berukuran 40x40, 100x100, 140x140, 200x200, 256x256 (piksel).

4. Kunci yang digunakan pada algoritma sebesar 128 bit
5. Software yang dipakai dalam implementasi algoritma RC6 adalah Matlab 2016b.
6. Tidak membahas serangan (threat) dari luar.

1.4 Metode Penelitian

Penelitian ini menerapkan beberapa metode penelitian yaitu sebagai berikut:

1. Studi Literatur
Pada tahap ini dilakukan pengumpulan referensi yang diperlukan oleh peneliti. Hal ini dilakukan agar memperoleh sebuah informasi dan data yang diperlukan untuk penulisan skripsi ini. Referensi yang digunakan dapat berupa buku, jurnal artikel, situs internet, maupun penelitian terdahulu yang berkaitan dengan penelitian ini.
2. Analisis Sistem
Pada tahap ini digunakan untuk mengolah data dari hasil studi literatur yang kemudian dilakukan sebuah analisis terhadap proses kerja penyembunyian dan enkripsi pesan dengan menggunakan kriptografi dan enkripsi RC6
3. Perancangan Sistem
Setelah pada tahapan analisis selesai, maka selanjutnya usulan kebutuhan akan diterjemahkan menjadi sistem informasi berbasis komputer yaitu dengan membuat rancangan sistem seperti bagan alir sistem dan desain antar muka pengguna.
4. Implementasi
Pada tahap implementasi ini dilakukan dengan menampilkan ke user hasil berupa sebuah aplikasi yang dapat mengamankan data digital image dengan menggunakan kriptografi RC6 dan Blum Blum Shub yang telah di implementasikan kedalam bahasa pemrograman Matlab.
5. Pengujian
Ditahap pengujian ini dilakukan suatu pengujian sebuah aplikasi untuk mengetahui apakah aplikasi tersebut sudah berjalan sesuai dengan tujuan penelitian atau tidak serta melakukan perbaikan jika terdapat error pada aplikasi tersebut.
6. Dokumentasi dan laporan akhir

Pada tahap yang terakhir ini dilakukan sebuah dokumentasi hasil sebuah analisa dan perancangan yang digunakan untuk menuangkan hasil penelitian tersebut kedalam laporan akhir dalam bentuk skripsi.

1.5 Sistematika Penulisan

Didalam penelitian ini, sistematika penulisan yang digunakan terbagi menjadi lima bab dengan susunan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan dasar-dasar dari penulisan laporan tugas akhir yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan, metode penelitian serta sistematika penulisan laporan tugas akhir.

BAB II LANDASAN TEORI

Bab ini membahas teori-teori yang berhubungan dengan topik penelitian, meliputi Blum Blum Shub dan kriptografi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini membahas tentang analisis proses enkripsi dan dekripsi algoritma RC6 dan Blum Blum Shub yang terdiri dari flowchart dan perancangan user interface

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang hasil implementasi dan pengujian sistem serta pembahasan dari hasil yang diperoleh sesuai dengan analisis dan perancangan sistem yang dilakukan sebelumnya.

BAB V PENUTUP

Bab ini membahas tentang kesimpulan yang diperoleh dari hasil penelitian serta saran-saran yang ditujukan bagi para pembaca dan pengembang sistem untuk penelitian selanjutnya.