PERBANDINGAN ALGORITMA KRIPTOGRAFI *RIJNDAEL* DAN *TWOFISH* PADA PENGAMANAN CITRA

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh :

FRESSY ARLIND
NIM : 09021381621106

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2019

LEMBAR PENGESAHAN TUGAS AKHIR

PERBANDINGAN ALGORITMA KRIPTOGRAFI *RIJNDAEL* DAN *TWOFISH* PADA PENGAMANAN CITRA

Oleh:

FRESSY ARLIND
NIM : 09021381621106

Palembang, Desember 2019

Pembimbing I,

Drs. Megah Mulya, M.T
NIP. 196602202006041001

Pembimbing II,

Osvari Arsalan, S.Kom., M.T.
NIP. 198211082012122001

Mengetahui,
Ketua Jurusan Teknik Informatika,

Rifkie Primartha, MT
NIP. 197706012009121004

TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Kamis tanggal 26 Desember 2019 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Fressy Arlind
NIM : 09021381621106
Judul : Perbandingan Algoritma Kriptografi *Rijndael* dan *Twofish* pada Pengamanan Citra

1. Pembimbing I

   Drs. Megah Mulya, M.T .....
   NIP. 196602202006041001

2. Pembimbing II

   Osvari Arsalan, S.Kom., M.T. .....
   NIP. 198806282018031001

3. Penguji I

   Alvi Syahrini Utami, M.Kom .....
   NIP. 197812222006042003

4. Penguji II

   Mastura Diana Marieska, S.T., M.T .....
   NIP. 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Rifkie Primartha, MT
NIP. 197706012009121004

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	:	Fressy Arlind
NIM	:	09021381621106
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Perbandingan Algoritma Kriptografi *Rijndael* dan *Twofish* pada Pengamanan Citra
Hasil Pengecekan Software *iThenticate/Turnitin*	:	8%

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 27 Desember 2019

Fressy Arlind
NIM. 09021381621106

MOTTO DAN PERSEMBAHAN

"To get a success, your courage must be greater than your fear"

"Never say
"Why I never get what I wanted?"!
It is possible that you dislike a thing which is good for you, and that you love a thing which is bad for you. But Allah knows, while you know not"

Kupersembahkan karya tulis ini kepada :

- *Kedua orangtuaku tercinta, kakak, dan keponakanku tersayang*
- *Keluarga besarku*
- *Teman - teman Tersayangku*
- *Fakultas Ilmu Komputer*
- *Universitas Sriwijaya*

ABSTRACT

The advancement of information technology will certainly have an impact on information security along with the ease of accessing media communication in this modern era. Cryptography provides the secure guarantee of information in order to avoid those impacts. The main characteristics of a good data encryption and decryption are security and speed. This study provides a comparative analysis of security and speed between two cryptography algorithms, Rijndael and Twofish, on image security with different mode of operations (ECB and CBC). Security analysis can be seen by the value of Avalanche Effect and speed analysis can be seen by the execution time of its algorithm. Based on the results of tests conducted, it is known that both the Rijndael and Twofish cryptographic algorithms both produce the avalanche effect in accordance with the Strict Avalanche Effect (SAC) which is close to 50%. In testing the Avalanche Effect changes in plainimage obtained the results of the Rijndael algorithm has the highest Avalanche Effect value of 52.8125% with CBC operating mode and small change pixel RGB value categories. Testing the Avalanche Effect changes to the key also outperformed by Rijndael with a value of 49,98619% with CBC operating mode. While for execution time, it can be concluded that the resolution and mode of operation has an influence on the execution time.

Keywords : Avalanche Effect, Execution Time, Rijndael, Twofish, Data Encryption and Decryption, ECB, CBC

ABSTRAK

Kemajuan teknologi informasi tentunya akan memberikan dampak bagi keamanan informasi seiring dengan mudahnya pengaksesan media komunikasi pada era modern ini. Kriptografi memberikan jaminan keamanan informasi yang dibutuhkan untuk menghindari dampak-dampak tersebut. Karakteristik utama dalam algoritma enkripsi dan dekripsi data yang baik adalah keamanan dan kecepatan. Penelitian ini memberikan analisis perbandingan keamanan dan kecepatan antar dua algoritma kriptografi, *Rjndael* dan *Twofish*, pada pengamanan citra dengan mode operasi yang berbeda (ECB dan CBC). Analisis keamanan dilihat dari nilai *Avalanche Effect* dan analisis kecepatan dilihat dari waktu eksekusi algoritma tersebut. Berdasarkan hasil pengujian yang dilakukan diketahui bahwa baik algoritma kriptografi *Rijndael* dan *Twofish* sama-sama menghasilkan nilai *avalanche effect* sesuai dengan *Strict Avalanche Effect* (SAC) yaitu mendekati 50%. Pada pengujian *Avalanche Effect* perubahan pada *plainimage* didapatkan hasil algoritma *Rijndael* memiliki nilai *Avalanche Effect* tertinggi sebesar 52.8125% dengan mode operasi CBC dan kategori nilai RGB pixel ubah kecil. Pengujian *Avalanche Effect* perubahan pada kunci juga diungguli oleh *Rijndael* dengan nilai sebesar 49.98619% dengan mode operasi CBC. Sedangkan utuk waktu eksekusi, didapatkan kesimpulan bahwa resolusi dan mode operasi memiliki pengaruh terhadap waktu eksekusi.

Kata Kunci : *Avalanche Effect*, Waktu Eksekusi, *Rijndael*, *Twofish*, Enkripsi dan Dekripsi Data, ECB, CBC

KATA PENGANTAR

Puji syukur kepada Allah atas berkat dan rahmat-Nya yang telah diberikan kepada Penulis sehingga dapat menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat guna menyelesaikan pendidikan program Strata-1 pada Fakultas Ilmu Komputer Program Studi Teknik Informatika di Universitas Sriwijaya.

Dalam menyelesaikan Tugas Akhir ini banyak pihak yang telah memberikan bantuan dan dukungan baik secara langsung maupun secara tidak langsung. Penulis ingin menyampaikan rasa terima kasih kepada:

1. Orang tuaku, Arsyad Hengry Bacik dan Herlinda, saudara-saudariku, Frizky Arlind, Freisha Arlind, dan Agung Hidayat, keponakanku, Aidan Ghally Hidayat, dan seluruh keluarga besarku yang selalu mendoakan serta memberikan dukungan baik moril maupun materil.
2. Bapak Jaidan Jauhari selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya, Bapak Rifkie Primartha selaku Ketua Jurusan Teknik Informatika, dan Ibu Hardini Novianti selaku Sekretaris Jurusan Teknik Informatika.
3. Bapak Megah Mulya selaku dosen pembimbing I dan Bapak Osvari Arsalan selaku pembimbing II yang telah membimbing, mengarahkan, dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
4. Ibu Yunita selaku dosen pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi penulis dalam proses perkuliahan dan pengerjaan Tugas Akhir.
5. Ibu Alvi Syahrini Utami selaku dosen penguji I, dan Ibu Mastura Diana Marieska selaku dosen penguji II yang telah memberikan masukan dan dorongan dalam proses pengerjaan Tugas Akhir.
6. Seluruh dosen Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Pak Tony, Mbak Anna, Mbak Wiwin dan seluruh staf tata usaha yang telah membantu dalam kelancaran proses administrasi dan akademik selama masa perkuliahan.

8. Sari Dwi Septiani dan Abdul Hafiz Muttaqien selaku sahabat yang telah menemani dan memotivasi selama proses menyelesaikan Tugas Akhir.
9. Teman-teman jurusan Teknik Informatika yang telah berbagi keluh kesah, motivasi, semangat, dan canda tawa selama masa perkuliahan.

Penulis menyadari dalam penyusunan Tugas Akhir ini masih terdapat banyak kekurangan disebabkan keterbatasan pengetahuan dan pengalaman, oleh karena itu kritik dan saran yang membangun sangat diharapkan untuk kemajuan penelitian selanjutnya. Akhir kata semoga Tugas Akhir ini dapat berguna dan bermanfaat bagi kita semua.

Palembang, Desember 2019

Fressy Arlind

DAFTAR ISI

Halaman

BAB III. METODOLOGI PENELITIAN

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR ALGORITMA

Halaman

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab ini diuraikan tentang pokok-pokok pikiran yang melandasi rencana skripsi. Pokok-pokok pikiran yang dimaksud diatas antara lain latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah.

1.2 Latar Belakang Masalah

Kriptografi merupakan cabang ilmu yang dikembangkan untuk mengamankan data atau informasi (Lusiana, 2011). Kemunculan kriptografi merupakan bentuk perhatian dari ancaman yang akan dihadapi seiring berkembangnya teknologi informasi. Ancaman-ancaman yang dimaksud adalah berbagai tindak kejahatan yang dapat mempengaruhi informasi dari segi kerahasiaan, otentikasi, integritas, dan ketersediaan data. Berbagai sektor seperti pemerintahan, militer, badan keuangan, rumah sakit, dan lain sebagainya menjadikan informasi sebagai peranan penting dalam menjalankan tugasnya (Kristoforus JB & Aditya BP, 2012). Hal tersebutlah yang membuat kriptografi mendapatkan perhatian lebih pada era digital seperti saat ini. Informasi yang diamankan bisa berupa teks, gambar, suara, video, dan lain sebagainya.

Salah satu algorirtma kriptografi adalah algoritma kriptografi kunci simetris. Algoritma kunci simetris ini menggunakan satu kunci yang sama dalam

proses enkripsi dan dekripsinya. Beberapa algoritma dari kunci simetris adalah DES, Blowfish, *Twofish*, LOKI, *Rijndael*, dan lain sebagainya. Algoritma *Rijndael* dan *Twofish* merupakan dua dari lima finalis dalam pemilihan standar *Advances Encryption Standard* (AES) sebagai pengganti *Data Encryption Standard* (DES) oleh *National Institute of Standard and Technology* (NIST). Algoritma *Rijndael* dan *Twofish* memiliki beberapa karakteristik yang sama dikarenakan ada beberapa syarat yang harus dipenuhi untuk menjadi kandidat AES yaitu merupakan algoritma kriptografi simetris berbasis *chiper block*, panjang kunci fleksibel (128, 192, dan 256 bit), ukuran block enkripsi yaitu 128 bit, dan mudah diimplementasikan. Tetapi, ada berbagai perbedaan juga antara kedua algoritma *Rijndael* dan *Twofish* seperti proses, kerumitan, waktu pemrosesan, dan lain-lain yang menyebabkan dipilihnya *Rijndael* sebagai pemenang AES.

Terdapat penelitian mengenai perbandingan antara algoritma kriptografi *rijndael* dan *twofish* untuk mengetahui perbedaan karakteristik antar kedua algoritma ini. Peneitian yang menganalisis perbandingan dengan parameter kecepatan, ukuran data setelah enkripsi, dan ketahanan terhadap serangan antara algoritma *Rijndael* dan *Twofish* pada file teks (Shulhan, 2018). Hasil dari penelitian tersebut adalah algoritma *rijndael* lebih unggul pada kecepatan dan ukuran data setelah enkripsi sedangkan algoritma *twofish* lebih unggul pada ketahanannya terhadap serangan. Hasil penelitian tersebut telah membuktikan bahwa algoritma pemenang (*Rijndael*) tidak selalu unggul dari algoritma finalis (*Twofish*). Oleh karena itu diperlukannya analisa lebih antara kedua algoritma *rijndael* dan *twofish*

untuk lebih memahami perbedaan karakteristik tersebut. Salah satu parameter pembanding yang dapat digunakan adalah pengukuran kekuatan.

Pengukuran kekuatan suatu algoritma kriptografi bisa dilakukan dengan cara melihat nilai perubahan kecil baik pada *plaintext* maupun kunci yang dapat mempengaruhi *chipertext* atau biasa disebut sebagai *avalanche effect* (Shi, Deng, & Yu, 2011). Kriteria algoritma kriptografi yang memiliki *Avalanche Effect* yang memuaskan adalah pada saat *chipertext* yang dihasilkan mengalami perubahan paling sedikit sebanyak 50% akibat terjadinya perubahan satu bit pada *plaintext* ataupun kunci (Bhoge & Chatur, 2014). Semakin tinggi nilai *avalanche effect* maka semakin bagus algoritma kriptografi tersebut.

Terdapat beberapa penelitian mengenai *avalanche effect* untuk mengukur keamanan suatu algoritma kriptografi. Salah satunya telah dilakukan oleh (Putra, Budiman, & Andini, 2015) yang menganalisis *avalanche effect* dari algoritma kriptografi *Rijndael* (AES) dengan mode *Electronic Code Book* (ECB). Dari hasil percobaan penelitian tersebut daoat dilihat nilai *avalanche effect* yang didapat baik dari perubahan *plaintext* ataupun kunci diatas 50%. Hal itu berarti untuk AES memiliki *avalanche effect* yang memuaskan. Efek yang lebih berpengaruh kuat adalah ketika terjadi perubahan pada *plaintext* dibandingkan adanya perubahan pada kunci. Tetapi, pada penelitian ini hanya menggunakan *plaintext* yang relatif pendek.

Penelitian lain mengenai *avalanche effect* juga telah dilakukan oleh (Mahamat et al. 2016) melakukan perbandingan nilai *avalanche effect* antara algoritma kriptografi AES, Blowfish, CAST-128, dan DES menggunakan mode

Electronic Code Book (ECB) dan *Cipher Block Chaining* (CBC). Hasil yang didapatkan adalah pada mode ECB dan CBC, DES memiliki *avalanche effec*t paling besar diantara yang lainnya. Akan tetapi untuk urutan keduanya, pada mode ECB AES memiliki *avalanche effect* yang paling tinggi dibandingkan Blowfish dan CAST-128. Sedangkan untuk mode CBC, nilai *avalanche effect* Blowfish lebih baik dari pada AES.

Berdasarkan penelitian yang telah dilakukan sebelumnya didapatkan hasil bahwa mode operasi ECB dan CBC akan memberikan hasil *avalanche effect* yang berbeda. Untuk itulah, pada penelitian ini akan dilakukan perbandingan algoritma *Rijndael* dan *Twofish* pada pengamanan citra dengan menggunakan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect* dan waktu eksekusi.

1.3 Rumusan Masalah

Berdasarkan latar belakang di atas dapat diidentifikasikan permasalahan yang muncul adalah bagaimana perbandingan keamanan antara algoritma *Rijndael* dan *Twofish* pada pengamanan citra dengan menggunakan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect*. Dari rumusan masalah yang telah dikemukakan, maka pertanyaan penelitian adalah bagaimana hasil perhitungan *avalanche effect* dan waktu eksekusi dari perbandingan algoritma kriptografi *Rijndael* dan *Twofish* pada pengamanan citra dengan mode operasi ECB dan CBC.

1.4 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dari penelitian ini adalah:

1. Mengembangkan perangkat lunak perbandingan algoritma kriptogafi *Rijndael* dan *Twofish* pada pengamanan citra.
2. Mengetahui nilai hasil perbandingan keamanan antara algoritma kriptografi *Rijndael* dan *Twofish* dengan mode operasi ECB dan CBC pada citra berdasarkan nilai *avalanche effect*.
3. Mengetahui nilai hasil perbandingan waktu eksekusi antara algoritma kriptografi *Rijndael* dan *Twofish* dengan mode operasi ECB dan CBC pada citra.

1.5 Manfaat Penelitian

Manfaat yang hendak dicapai dalam pelaksanaan penelitian ini adalah:

1. Mengetahui mode operasi yang lebih tepat digunakan pada algoritma kriptografi *rijndael* dan *twofish* sehingga memberikan nilai *avalanche effect* yang tinggi.
2. Mengetahui pengaruh resolusi citra terhadap perubahan waktu eksekusi.

1.6 Batasan Masalah

Karena keterbatasan waktu dan pengetahuan penulis, maka ruang lingkup permasalahan dalam penelitian ini dibatasi pada bidang kajian yang dibahas yaitu:

1. Algoritma kriptografi yang dibandingkan adalah *rijndael* dan *twofish* dengan panjang kunci 128 bit.

2. Data yang digunakan berupa citra bitmap dengan resolusi 32 x 32, 128 x 128, 256 x 256, 512 x 512, dan 1024 x 1024.
3. Satuan untuk nilai *avalanche effect* menggunakan persen (%).
4. Mode operasi yang digunakan adalah ECB dan CBC.
5. Proses enkripsi dekripsi *block* dilakukan menggunakan *library Bouncy Castle* yang di-*support* oleh *Australian Charitable Organization* yaitu *Legion of the Bouncy Castle* Inc.

1.7 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini diuraikan tentang pokok-pokok pikiran yang melandasi rencana skripsi. Pokok-pokok pikiran yang dimaksud diatas antara lain latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti citra bitmap, kriptografi, enkripsi dan dekripsi data, *stream* dan *blok ci*pher, mode operasi, *S-Box*, algoritma *rijndael*, Matriks *Maximum Distances Separable* (MDS), *Pseudo-Hadamard Transformation*

(PHT), jaringan feistel, fungsi f, fungsi g, algoritma *twofish*, dan *avalanche effect*, serta penelitian terdahulu yang relevan.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dijelaskan data yang akan digunakan pada penelitian ini dan bagaimana cara pengumpulan datanya. Lalu, akan dijelaskan tahapan penelitian yang akan diimplementasikan, metode pengembangan perangkat lunak serta manajemen proyek penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini diuraikan tahapan yang dilakukan dalam proses pengembangan perangkat lunak yang merupakan alat penelitian yang digunakan untuk melakukan perbandingan algoritma kriptografi *Rijndael* dan *Twofish* dalam pengaman citra dengan menggunakan metode *Rational Unified Process* (RUP).

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini akan diuraikan hasil pengujian dan analisis hasil pengujian dari pengembangan perangkat lunak.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini akan dijabarkan kesimpulan penelitian dan saran yang diharapkan dapat dijadikan sebagai acuan untuk penelitian lain di bidang yang sama kedepannya.

1.8 Kesimpulan

Penelitian yang akan dijadikan rencana tugas akhir adalah penelitian tentang perbandingan algoritma *twofish* dan *rijndael* pada pengamangan citra dengan mode operasi ECB dan CBC berdasarkan nilai *avalanche effect* dan waktu eksekusi.

DAFTAR PUSTAKA

Bhoge, Jayant P, dan Prashant N Chatur. 2014. "Avalanche Effect of AES Algorithm." *International Journal of Computer Science and Information Technologies* 5 (3): 3101–3.

Kristoforus JB, R., dan Stefanus Aditya BP. 2012. "Implementasi Algoritma Rijndael Untuk Enkripsi Dan Deskripsi Pada Citra Digital" 2012 (Snati): 15–16.

Lusiana, Veronica. 2011. "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128." *Jurnal Dinamika Informatika* 3: 79–84. https://doi.org/10.1108/02683940510579731.

Mahamat, Youssouf, Siti Hajar Othman, Maheyzah Siraj, dan Herve Nkiama. 2016. "Comparative Study Of AES , Blowfish , CAST-128 And DES Encryption Algorithm International Organization of Scientific Research International Organization of Scientific Research" 06 (06): 1–7.

Muhathir, Muhathir. 2019. "Perbandingan Algoritma Blowfish Dan Twofish Untuk Kriptografi File Gambar." *Journal of Informatics and Telecommunication Engineering* 2 (1): 23. https://doi.org/10.31289/jite.v2i1.1673.

Putra, Fadhlan, Gelar Budiman, dan Nur Andini. 2015. "COMPARATION AND ANALYSIS OF PERFORMANCE OF ENCRYPTION- DECRYPTION OF TEXT USING AES ALGORITHM AND MODIFIED AES BASED ON ANDROID" 2 (2): 3022–30.

Sharif, Suhaila Orner, dan S P Mansoor. 2010. "Performance Analysis of Stream and Block Cipher Algorithms," 522–25.

Shi, Hui, Yuanqing Deng, dan Guan Yu. 2011. "Analysis of the Avalanche Effect of the AES S Box." *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce, AIMSEC 2011 - Proceedings*, 5425–28. https://doi.org/10.1109/AIMSEC.2011.6009935.

Shulhan, Izzat. 2018. "Analisis Perbandingan Antara Algoritma Rijndael Dan Algoritma Twofish Dalam Penyandian Teks." *Jurnal Teknik Informatika Unika St. Thomas (JTIUST)* 03.

Silva, Mathieu Da, Emanuele Valea, Marie-lise Flottes, Sophie Dupuis, Giorgio Di Natale, dan Bruno Rouzeyre. 2018. "Encryption of Test Data : Which Cipher Is Better ?" *2018 14th Conference on Ph.D. Research in Microelectronics and Electronics (PRIME)*, 85–88.