

**SISTEM PENGAMANAN PESAN DENGAN METODE KRIPTOGRAFI  
RC4 DAN STEGANOGRAFI LEAST SIGNIFICANT BIT BERBASIS  
ANDROID**

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



Oleh:

ANANG NUGRAHA

NIM : 09021381722106

**Jurusan Teknik Informatika  
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA  
2021**

**LEMBAR PENGESAHAN TUGAS AKHIR**

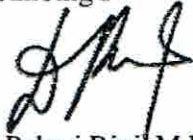
**SISTEM PENGAMANAN PESAN DENGAN METODE KRIPTOGRAFI  
RC4 DAN STEGANOGRAFI LEAST SIGNIFICANT BIT BERBASIS  
ANDROID**

Oleh:

**Anang Nugraha**  
NIM: 09021381722106

Palembang, Juni 2021

Pembimbing I



**Dian Palupi Rini, M.Kom., Ph.D.**  
NIP. 197802232006042002

Pembimbing II,



**Kanda Januar Miraswan, M.T.**  
NIP. 199001092019031012

Mengetahui,  
Ketua Jurusan Teknik Informatika



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



## TANDA LULUS UJIAN SIDANG TUGAS AKHIR

Pada hari Jumat tanggal 07 Mei 2021 telah dilaksanakan ujian sidang tugas akhir oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Anang Nugraha  
NIM : 09021381722106  
Judul Skripsi : Sistem Pengamanan Pesan dengan Metode Kriptografi RC4 dan Steganografi Least Significant Bit Berbasis Android

1. Pembimbing I

Dian Palupi Rini, M.Kom., Ph.D.  
NIP. 197802232006042002



2. Pembimbing II

Kanda Januar Miraswan, M.T.  
NIP. 199001092019031012



3. Penguji I

Julian Supardi, M.T.  
NIP. 197207102010121001




4. Penguji II

Muhammad Ali Buchari., M.T.  
NIP. 198803302019031007



Mengetahui,  
Ketua Jurusan Teknik Informatika

  
Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003



## HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Anang Nugraha

NIM : 09021381722106

Program Studi : Teknik Informatika

Judul Skripsi : Sistem Pengamanan Pesan dengan Metode Kriptografi RC4 dan  
Steganografi Least Significant Bit Berbasis Android

Hasil Pengecekan Software *iThenticate/Turnitin* : 12%

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, 01 Juni 2021



Anang Nugraha

NIM. 09021381722106

## **MOTTO DAN PERSEMBAHAN**

MOTTO:

“Stay Hungry, Stay Foolish”

-Steve Jobs-

“Learn from yesterday, live for today, hope for tomorrow.

The important thing is not to stop questioning.”

-Albert Einstein-

**Kupersembahkan karya tulis ini kepada :**

- **Keluargaku Tercinta**
- **Sahabat-sahabatku**
- **Fakultas Ilmu Komputer,  
Universitas Sriwijaya**

**Message Security System using the RC4 Cryptography and Least Significant Bit Steganography Methods Based on Android**

By :  
**Anang Nugraha**  
**09021381722106**

**ABSTRACT**

The security of information is an essential aspect that must be considered these days, especially for private or confidential information, security can be done in several ways, including cryptographic and steganographic methods, which have their respective advantages and disadvantages, so we can combine the two methods to get a higher level of security. This study is based on the process of encrypting text messages using the RC4 cryptographic algorithm and inserted it into the image media using the LSB method. There are 3 images with 128X128, 256X256, 512X512, 1920X1920, and 2400X2400 resolutions each with a total of 15 images and also ASCII messages with a length of 100, 250, and 500 characters that will be inserted in each image for testing purpose. The stego image quality is based on the PSNR score. On this study the PSNR score on all test images and texts delivers the lowest score of 68.319 and the highest score of 76.921, which meets the criteria as a good stego image. Besides that, the RC4 cryptographic algorithm can also deliver a good Avalanche Effect with a 46.25% of average score, and the combination of the RC4 cryptography algorithm with the LSB steganography method has very small differences in execution time in each test scheme.

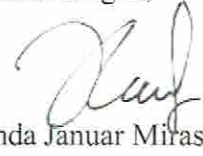
**Keywords:** Cryptography, Steganography, RC4, LSB, PSNR, Avalanche Effect

Palembang, 01 Juni 2021

Pembimbing I

Pembimbing II,

  
Dian Palupi Rini, M.Kom., Ph.D.  
NIP. 197802232006042002

  
Kanda Januar Miraswan, M.T.  
NIP. 199001092019031012

Mengetahui,  
Ketua Jurusan Teknik Informatika

  
Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003

## Sistem Pengamanan Pesan dengan Metode Kriptografi RC4 dan Steganografi Least Significant Bit Berbasis Android

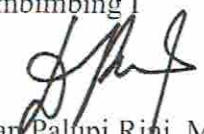
Oleh :  
Anang Nugraha  
09021381722106

### ABSTRAK

Keamanan merupakan aspek penting yang harus diperhatikan dalam menyampaikan informasi di masa sekarang, terutama informasi yang bersifat pribadi atau rahasia, pengamanan dapat dilakukan dengan beberapa cara diantaranya dengan kriptografi dan steganografi yang memiliki kelebihan dan kekurangannya masing-masing, maka di gabungkanlah kedua metode tersebut untuk mendapatkan tingkat keamanan yang lebih tinggi. Penelitian ini berfokus kepada proses enkripsi pesan teks menggunakan kriptografi RC4 yang kemudian disisipkan ke dalam media citra penampung menggunakan metode LSB. Terdapat citra dengan resolusi 128X128, 256X256, 512X512, 1920X1920, dan 2400X2400 sebanyak masing-masing 3 citra dengan total 15 citra dan juga pesan ASCII dengan Panjang 100, 250 dan 500 karakter yang akan disisipkan pada citra penampung pengujian. Kualitas citra hasil penyisipan diukur berdasarkan nilai PSNR yang dihasilkan dari semua citra dan teks pengujian dengan nilai terendah 68.319 dan tertinggi 76.921 yang memenuhi kriteria citra stego yang baik, selain itu algoritma kriptografi RC4 juga dapat menghasilkan nilai Avalanche Effect yang cukup baik dengan rata-rata 46.25% dan skema penggabungan ini memiliki perbedaan waktu eksekusi yang cenderung sangat sedikit pada masing-masing skema pengujian.

**Kata Kunci:** Kriptografi, Steganografi, RC4, LSB, PSNR, Avalanche Effect

Pembimbing I

  
Dian Palupi Rini, M.Kom., Ph.D.  
NIP. 197802232006042002


Palembang, 01 Juni 2021

Pembimbing II,

  
Kanda Januar Miraswan, M.T.  
NIP. 199001092019031012

Mengetahui,  
Ketua Jurusan Teknik Informatika



  
Alvi Syahrini Utami, M.Kom.  
NIP. 197812222006042003

## KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya yang telah melimpahkan rahmat dan karunianya kepada Penulis sehingga mampu menyelesaikan Tugas Akhir ini dengan baik. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk 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 tidak langsung. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Orang tuaku tercinta, Zahirudin dan Susmawarna, saudariku, Tiah Seftiani, A.Md.Rad. dan Lega Aryanti, A.Md.Far., kakak ipar dan juga keponakanku yang selalu memberikan semangat, doa, dan dukungan baik secara moril maupun materil.
2. Bapak Jaidan Jauhari, M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya beserta jajarannya. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika beserta jajarannya.
3. Ibu Dian Palupi Rini selaku dosen pembimbing I dan Bapak Kanda Januar Miraswan selaku pembimbing II yang telah membimbing, mengarahkan dan memberikan motivasi kepada penulis dalam perkuliahan dan pengerjaan Tugas Akhir.
4. Ibu Dian Palupi Rini selaku pembimbing akademik, yang telah membimbing, mengarahkan dan memberikan motivasi kepada penulisan dalam proses perkuliahan dari awal sampai akhir.
5. Seluruh dosen dan Civitas Akademika Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberikan banyak sekali ilmu, pengalaman, dan motivasi kepada penulis dalam perkuliahan.



6. Teman-teman seperjuangan di kelas TI BIL B 2017 yang semuanya selalu menemani hari-hari perkuliahan.
7. Sahabat-sahabat terbaikku Rafly, Opang, Gumay, Adrian, Ryzki, Aldi Ariqi, Aldi Riansyah, Robi, Iman dan mereka yang namanya tidak bisa disebutkan satu persatu yang selalu menemani hari-hariku baik didalam maupun diluar perkuliahan.
8. Dan juga, seluruh pihak yang telah membantu dalam penyusunan dan penyempurnaan tugas akhir ini yang tidak dapat disebutkan satu persatu.

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

Palembang, Juni 2021

Penulis

Anang Nugraha

## DAFTAR ISI

|  |             |
|--|-------------|
| <b>HALAMAN JUDUL .....</b>                     | <b>i</b>    |
| <b>HALAMAN PENGESAHAN.....</b>                 | <b>ii</b>   |
| <b>HALAMAN PERSETUJUAN KOMISI PENGUJI.....</b> | <b>iii</b>  |
| <b>HALAMAN PERNYATAAN.....</b>                 | <b>ii</b>   |
| <b>HALAMAN MOTTO DAN PERSEMBAHAN .....</b>     | <b>ii</b>   |
| <b>ABSTRACT .....</b>                          | <b>iii</b>  |
| <b>ABSTRAK .....</b>                           | <b>vii</b>  |
| <b>KATA PENGANTAR.....</b>                     | <b>viii</b> |
| <b>DAFTAR ISI.....</b>                         | <b>x</b>    |
| <b>DAFTAR TABEL .....</b>                      | <b>xiii</b> |
| <b>DAFTAR GAMBAR.....</b>                      | <b>xiv</b>  |
| <b>DAFTAR ALGORITMA .....</b>                  | <b>xv</b>   |
| <br>   |             |
| <b>BAB I PENDAHULUAN.....</b>                  | <b>I-1</b>  |
| 1.1    Pendahuluan .....                       | I-1         |
| 1.2    Latar Belakang .....                    | I-1         |
| 1.3    Rumusan Masalah .....                   | I-3         |
| 1.4    Tujuan Penelitian .....                 | I-4         |
| 1.5    Manfaat Penelitian .....                | I-5         |
| 1.6    Batasan Masalah .....                   | I-5         |
| 1.7    Sistematika Penulisan .....             | I-6         |
| 1.8    Kesimpulan .....                        | I-6         |
| <br>   |             |
| <b>BAB II KAJIAN LITERATUR .....</b>           | <b>II-1</b> |
| 2.1    Pendahuluan .....                       | II-1        |
| 2.2    Landasan Teori.....                     | II-1        |
| 2.2.1    Kriptografi.....                      | II-1        |
| 2.2.2    Kriptografi RC4 .....                 | II-3        |
| 2.2.3    Steganografi .....                    | II-6        |

|   |   |              |
|---|---|--------------|
| 2.2.4                                       | Steganografi Algoritma <i>Least Significant Bit</i> (LSB) ..... | II-7         |
| 2.2.5                                       | Mean Squared Error dan Peak Signal to Noise Ratio .....         | II-9         |
| 2.2.6                                       | Avalanche Effect.....   | II-10        |
| 2.2.7                                       | Rational Unified Process (RUP) .....                            | II-10        |
| 2.3   | Penelitian Lain Yang Relevan.....                               | II-11        |
| 2.4   | Kesimpulan .....  | II-13        |
| <b>BAB III METODOLOGI PENELITIAN .....</b>  |   | <b>III-1</b> |
| 3.1   | Pendahuluan .....   | III-1        |
| 3.2   | Pengumpulan Data .....  | III-1        |
| 3.2.1                                       | Jenis Data .....  | III-1        |
| 3.2.2                                       | Sumber Data.....  | III-2        |
| 3.3   | Tahapan Penelitian.....   | III-2        |
| 3.3.1                                       | Kerangka Kerja Penelitian .....                                 | III-3        |
| 3.3.2                                       | Kriteria Pengujian .....  | III-5        |
| 3.3.3                                       | Format Data Pengujian.....                                      | III-7        |
| 3.3.4                                       | Alat yang Digunakan dalam Pelaksanaan Penelitian.....           | III-9        |
| 3.3.5                                       | Pengujian Penelitian.....                                       | III-9        |
| 3.3.6                                       | Analisa Hasil Pengujian dan Membuat Kesimpulan Penelitian... .. | III-10       |
| 3.4   | Metode Pengembangan Perangkat Lunak.....                        | III-10       |
| 3.4.1                                       | Fase Insepsi .....  | III-10       |
| 3.4.2                                       | Fase Elaborasi .....  | III-11       |
| 3.4.3                                       | Fase Konstruksi.....  | III-11       |
| 3.4.4                                       | Fase Transisi .....   | III-12       |
| 3.5   | Manajemen Proyek Penelitian .....                               | III-12       |
| <b>BAB IV REKAYASA PERANGKAT LUNAK.....</b> |   | <b>IV-1</b>  |
| 4.1   | Pendahuluan .....   | IV-1         |
| 4.2   | Fase Insepsi .....  | IV-1         |
| 4.2.1                                       | Pemodelan Bisnis.....   | IV-1         |
| 4.2.2                                       | Kebutuhan Sistem .....  | IV-2         |
| 4.2.3                                       | Analisis dan Desain.....  | IV-3         |
| 4.2.4                                       | Implementasi.....   | IV-5         |

|   |  |              |
|---|--|--------------|
| 4.3   | Fase Elaborasi .....                       | IV-5         |
| 4.3.1   | Pemodelan Bisnis .....                     | IV-5         |
| 4.3.2   | Kebutuhan Sistem .....                     | IV-19        |
| 4.3.3   | Analisis dan Desain.....                   | IV-19        |
| 4.3.4   | Implementasi.....                          | IV-20        |
| 4.3.1   | Fase Konstruksi.....                       | IV-20        |
| 4.4.1   | Kebutuhan .....                            | IV-21        |
| 4.4.2   | Analisa dan Desain.....                    | IV-22        |
| 4.4.3   | Implementasi .....                         | IV-25        |
| 4.4   | Fase Transisi .....                        | IV-27        |
| 4.5.1   | Pemodelan Bisnis.....                      | IV-27        |
| 4.5.2   | Kebutuhan .....                            | IV-27        |
| 4.5.3   | Analisis dan Desain.....                   | IV-27        |
| 4.5.4   | Implementasi.....                          | IV-30        |
| 4.5   | Kesimpulan .....                           | IV-39        |
| <b>BAB V HASIL DAN ANALISIS PENELITIAN.....</b> |  | <b>V-1</b>   |
| 5.1   | Pendahuluan .....                          | V-1          |
| 5.2   | Data Hasil Percobaan Penelitian .....      | V-1          |
| 5.2.1   | Konfigurasi Percobaan.....                 | V-1          |
| 5.2.2   | Data Hasil Pengujian PSNR.....             | V-2          |
| 5.2.3   | Data Hasil Pengujian Avalanche Effect..... | V-12         |
| 5.2.4   | Data Hasil Pengujian Waktu Eksekusi.....   | V-14         |
| 5.3   | Analisis Hasil Penelitian .....            | V-16         |
| 5.4   | Kesimpulan .....                           | V-20         |
| <b>BAB VI KESIMPULAN DAN SARAN .....</b>        |  | <b>VI-1</b>  |
| 6.1   | Pendahuluan .....                          | VI-1         |
| 6.2   | Kesimpulan .....                           | VI-1         |
| 6.3   | Saran.....                                 | VI-2         |
| <b>DAFTAR PUSTAKA.....</b>                      |  | <b>xvi</b>   |
| <b>LAMPIRAN.....</b>                            |  | <b>xviii</b> |

## DAFTAR TABEL

|   |       |
|---|-------|
| <b>Tabel III-1.</b> Rancangan Tabel Hasil Pengujian MSE dan PSNR Citra Stego ..                             | III-7 |
| <b>Tabel III- 2.</b> Rancangan Tabel Hasil Pengujian Avalanche Effect.....                                  | III-7 |
| <b>Tabel III- 3.</b> Rancangan Tabel Hasil Pengujian Waktu Eksekusi Encoding -<br>Enkripsi .....            | III-8 |
| <b>Tabel III- 4.</b> Rancangan Tabel Hasil Pengujian Waktu Eksekusi Decoding -<br>Dekripsi.....             | III-8 |
| <b>Tabel IV- 1</b> Kebutuhan Fungsional Perangkat Lunak.....  | IV-2  |
| <b>Tabel IV- 2</b> Kebutuhan Non Fungsional Perangkat Lunak.....  | IV-3  |
| <b>Tabel IV- 3</b> Definisi Aktor.....  | IV-7  |
| <b>Tabel IV- 4</b> Definisi Use-Case.....   | IV-7  |
| <b>Tabel IV- 5</b> Skenario Use-Case Melakukan Penyisipan Pesan.....  | IV-8  |
| <b>Tabel IV- 6</b> Skenario Use-Case Melakukan Pengekstraksian Pesan .....                                  | IV-9  |
| <b>Tabel IV- 7</b> Skenario Use-Case Menghitung nilai PSNR.....   | IV-11 |
| <b>Tabel IV- 8</b> Skenario Use Case Menghitung Avalanche Effect .....                                      | IV-12 |
| <b>Tabel IV- 9.</b> Spesifikasi kebutuhan lingkungan pengembangan perangkat keras &<br>perangkat lunak..... | IV-22 |
| <b>Tabel IV- 10.</b> Daftar Implementasi Kelas .....  | IV-26 |
| <b>Tabel IV- 11.</b> Skenario pengujian melakukan enkripsi pesan.....                                       | IV-28 |
| <b>Tabel IV- 12.</b> Skenario pengujian melakukan dekripsi pesan.....                                       | IV-28 |
| <b>Tabel IV- 13.</b> Skenario pengujian melakukan penyisipan pesan .....                                    | IV-28 |
| <b>Tabel IV- 14.</b> Skenario pengujian melakukan ekstraksi pesan .....                                     | IV-29 |
| <b>Tabel IV- 15.</b> Skenario pengujian melakukan perhitungan PSNR. ....                                    | IV-29 |
| <b>Tabel IV- 16.</b> Skenario pengujian menghitung Avalanche Effect .....                                   | IV-29 |
| <b>Tabel IV- 17.</b> Hasil Pengujian Use Case Penyisipan Pesan.....   | IV-33 |
| <b>Tabel IV- 18.</b> Hasil Pengujian Use Case Ekstraksi Pesan .....   | IV-34 |
| <b>Tabel IV- 19.</b> Hasil Pengujian Use Case Encoding .....  | IV-35 |
| <b>Tabel IV- 20.</b> Hasil Pengujian Use Case Decoding .....  | IV-36 |
| <b>Tabel IV- 21.</b> Hasil Pengujian Use Case Menghitung Nilai PSNR .....                                   | IV-37 |
| <b>Tabel IV- 22.</b> Hasil Pengujian Use Case Menghitung Avalanche Effect .....                             | IV-38 |
| <b>Tabel V- 1</b> Hasil Pengujian MSE dan PSNR .....  | V-2   |
| <b>Tabel V- 2</b> Hasil Pengujian Avalanche Effect RC4.....   | V-12  |
| <b>Tabel V- 3</b> Hasil Pengujian Waktu Eksekusi Skema Enkripsi-Encoding.....                               | V-14  |
| <b>Tabel V- 4</b> Hasil Pengujian Waktu Eksekusi Skema Decoding-Dekripsi.....                               | V-15  |

## DAFTAR GAMBAR

|  |        |
|--|--------|
| <b>Gambar II-1.</b> Skema enkripsi dan dekripsi sederhana (Mukhtar, 2018)..... | II-3   |
| <b>Gambar II-2.</b> Skema proses algoritma RC4.....                            | II-4   |
| <b>Gambar II-3.</b> Skema encoding dan decoding (Endang & Melisa, 2016).....   | II-7   |
| <b>Gambar II-4</b> MSB dan LSB (Endang & Melisa, 2016) .....                   | II-7   |
| <b>Gambar II-5</b> Diagram Proses RUP (Kruchten, 2003).....                    | II-11  |
| <b>Gambar III-1</b> Kerangka Kerja proses Enkripsi – Encoding.....             | III-4  |
| <b>Gambar III-2</b> Kerangka Kerja proses Dekripsi – Decoding .....            | III-4  |
| <b>Gambar III-3</b> Gantt Chart Penjadwalan Penelitian .....                   | III-17 |
| <b>Gambar IV- 1</b> Diagram Alir Penyisipan Pesan .....                        | IV-4   |
| <b>Gambar IV- 2</b> Diagram Alir Pengekstraksian Pesan.....                    | IV-4   |
| <b>Gambar IV- 3</b> Diagram Alir Menghitung Avalanche Effect.....              | IV-5   |
| <b>Gambar IV- 4</b> Diagram Use Case Fase Elaborasi .....                      | IV-6   |
| <b>Gambar IV- 5</b> Diagram Aktivitas Penyisipan Pesan.....                    | IV-14  |
| <b>Gambar IV- 6</b> Diagram Aktivitas Pengekstraksian Pesan .....              | IV-15  |
| <b>Gambar IV- 9</b> Diagram Aktivitas Menghitung nilai PSNR .....              | IV-16  |
| <b>Gambar IV- 10</b> Diagram Aktivitas Menghitung Avalanche Effect .....       | IV-16  |
| <b>Gambar IV- 11.</b> Diagram Sekuensial Melakukan Penyisipan Pesan .....      | IV-17  |
| <b>Gambar IV- 12.</b> Diagram Sekuensial Melakukan Ekstraksi Pesan.....        | IV-21  |
| <b>Gambar IV- 15.</b> Diagram Sekuensial Melakukan Perhitungan PSNR.....       | IV-18  |
| <b>Gambar IV- 16.</b> Diagram Sekuensial Menghitung Avalanche Effect.....      | IV-19  |
| <b>Gambar IV- 17.</b> Diagram Kelas .....                                      | IV-21  |
| <b>Gambar IV- 18.</b> Rancangan Antarmuka Menu Encoding .....                  | IV-23  |
| <b>Gambar IV- 19.</b> Rancangan Antarmuka Menu Decoding.....                   | IV-24  |
| <b>Gambar IV- 20.</b> Rancangan Antarmuka Menghitung Avalanche Effect .....    | IV-24  |
| <b>Gambar IV- 21.</b> Tampilan Antarmuka Menu Encoding .....                   | IV-30  |
| <b>Gambar IV- 22.</b> Tampilan Antarmuka Menu Decoding .....                   | IV-31  |
| <b>Gambar IV- 23.</b> Tampilan Antarmuka Menu Perhitungan Avalanche Effect     | IV-32  |
| <b>Gambar V-1</b> Nilai Rata-Rata MSE.....                                     | V-17   |
| <b>Gambar V- 2</b> Nilai Rata-Rata PSNR.....                                   | V-17   |
| <b>Gambar V- 3</b> Grafik Nilai Avalanche Effect RC4 .....                     | V-18   |
| <b>Gambar V- 4</b> Nilai Rata-Rata Waktu Eksekusi Skema Enkripsi-Encoding....  | V-19   |
| <b>Gambar V- 5</b> Nilai Rata-Rata Waktu Eksekusi Skema Decoding-Dekripsi ...  | V-19   |

## DAFTAR ALGORITMA

|  |      |
|--|------|
| <b>Algoritma II-1</b> <i>Key Scheduling Algorithm</i> .....                  | II-5 |
| <b>Algoritma II-2</b> <i>Pseudo Random Generation Algorithm (PRGA)</i> ..... | II-5 |
| <b>Algoritma II-3</b> Encoding Algoritma Steganografi LSB.....               | II-8 |
| <b>Algoritma II-4</b> Decoding Algoritma Steganografi LSB.....               | II-8 |

# **BAB I**

## **PENDAHULUAN**

### **1.1 Pendahuluan**

Pada bab pendahuluan akan membahas latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan. Bab ini akan memaparkan penjelasan umum yang mencakup keseluruhan penelitian.

### **1.2 Latar Belakang**

Keamanan merupakan salah satu aspek penting yang harus diperhatikan terutama dalam menyampaikan sebuah informasi. Perkembangan alat komunikasi saat ini membuat banyak orang saling bertukar informasi melalui internet. Mengiriman informasi tanpa melakukan pengamanan terlebih dahulu bisa beresiko membuat informasi dapat dicuri oleh orang yang tidak bertanggung jawab Sehingga dibutuhkan pengamanan pada informasi sebelum dikirimkan (Akash *et al.*, 2018). Pengamanan data dapat dilakukan dengan berbagai cara seperti kriptografi dan steganografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan sehingga tidak dapat dimengerti oleh pihak yang tidak bertanggung jawab (Singhal & Raina, 2011).



Banyak algoritma kriptografi yang dapat digunakan untuk melakukan pengamanan pesan, salah satunya adalah RC4, Algoritma RC4 adalah algoritma yang dirancang oleh Ron Rivest yang berasal dari laboratorium RSA. Algoritma RC4 sendiri merupakan kriptografi kunci simetris stream cipher yang proses enkripsi dan dekripsinya dilakukan satu per satu bit atau bit per bit (Pratama & Sari, 2019). Dalam tulisan sebelumnya yang ditulis oleh Nidhi Singhal dan J.P.S.Raina (2011) yang berjudul “*Comparative Analysis of AES and RC4 Algorithms for Better Utilization*” menyebutkan bahwa algoritma stream cipher RC4 masih terbilang aman dan bisa lebih cepat dari algoritma block cipher dalam beberapa skenario percobaan.

Dengan menggunakan metode kriptografi saja hasil enkripsi data dapat dicurigai oleh orang yang membacanya, dan beresiko mendapat upaya serangan untuk mengungkap data tersebut oleh *cryptanalyst* melalui berbagai macam metode penyerangan (Kamble & Meshram, 2012). Sehingga perlu adanya suatu metode lagi agar data hasil enkripsi tersebut terlihat seperti data normal (pesan seperti tersembunyi) sehingga menghindari penyerangan.

Salah satu ilmu menyembunyikan pesan sedemikian rupa dengan suatu teknik tertentu sehingga keberadaan dari pesan tersebut tidak terdeteksi oleh indera manusia adalah Steganografi (Ricky *et al.*, 2018), salah satu teknik steganografi adalah *Least Significant Bit (LSB)* yang menggunakan cara penyisipan pada bit rendah atau bit yang paling kanan pada data pixel yang menyusun file tersebut, Penelitian sebelumnya terkait dengan Steganografi LSB pada media citra dilakukan oleh Muhammad Ricky *et al.* (2018) dengan judul “Analisis Steganography Pada

Citra Digital dengan Menggunakan Metode Least Significant Bit Berbasis Mobile Android” menyebutkan bahwa teknik tersebut dapat menghasilkan citra stego yang memenuhi kriteria sebagai steganografi yang dikatakan baik yakni memiliki imperceptibility (keberadaan pesan yang disisipkan pada media citra stego secara kasat mata tidak dapat terlihat), fidelity (kualitas dari citra yang telah disisipi pesan tidak berubah) dan memiliki recovery (citra stego yang terdapat pesan didalamnya dapat diekstrak kembali). Tetapi metode steganografi memiliki kelemahan, yaitu setelah pihak ketiga dapat mengekstrak pesan dari media steganografi, maka pesan tersebut akan langsung didapatkan. Untuk memperbaiki kekurangan tersebut maka di rancanglah kombinasi kedua metode kriptografi dan steganografi tersebut untuk meningkatkan level keamanan data. (Atee *et al.*, 2014)

Pada penelitian ini dirancang sebuah aplikasi yang dapat memenuhi kebutuhan pengamanan data seperti yang disebutkan diatas, yaitu pengamanan pesan teks yang di enkripsi menggunakan algoritma kriptografi *RC4* ke dalam sebuah citra digital menggunakan metode Steganografi *Least Significant Bit* (LSB) berbasis Android. Sehingga diharapkan aplikasi ini dapat menjadi salah satu pilihan untuk mengamankan data teks yang nantinya dapat dikirimkan bahkan di dalam sebuah lingkungan yang rentan terhadap berbagai macam serangan terhadap informasi.

## **1.1 Rumusan Masalah**

Berdasarkan rumusan masalah pada latar belakang diatas, maka pertanyaan penelitian pada permasalahan ini adalah sebagai berikut:

1. Bagaimana kualitas citra stego setelah proses penyematan pesan terenkripsi ke dalam citra penampung dengan pengkombinasian algoritma kriptografi RC4 dan steganografi LSB?
2. Bagaimana tingkat keamanan dan kualitas algoritma kriptografi RC4 sebagai algoritma untuk melakukan enkripsi pesan?
3. Bagaimana performansi algoritma kriptografi RC4 dan steganografi LSB pada proses enkripsi-encoding dan dekripsi-decoding.

## 1.2 Tujuan Penelitian

Tujuan pada penelitian ini adalah sebagai berikut :

1. Melakukan pengembangan perangkat lunak berbasis Android yang mengimplementasikan skema penggabungan algoritma Kriptografi RC4 dan Steganografi *Least Significant Bit* (LSB);
2. Melakukan perhitungan terhadap aspek kualitas citra steganografi yang meliputi perhitungan pada nilai *Mean Square Error* (MSE) dan nilai *Peak Signal-to-Noise Ratio* (PSNR);
3. Melakukan pengukuran kualitas dan kekuatan algoritma kriptografi RC4 berdasarkan peninjauan dari *Avalanche Effect*;
4. Melakukan pengukuran aspek kecepatan komputasi melalui pengukuran waktu eksekusi dari proses enkripsi-encoding dan dekripsi-decoding.

### 1.3 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Menghasilkan sebuah perangkat lunak berbasis Android yang dapat mengimplementasikan skema penggabungan algoritma Kriptografi RC4 dan Steganografi *Least Significant Bit* (LSB) sebagai pengamanan pesan;
2. Mengetahui kualitas citra stego berdasarkan hasil pengujian dari skema penggabungan algoritma Kriptografi RC4 dan Steganografi *Least Significant Bit* (LSB).
3. Mengetahui tingkat keamanan algoritma kriptografi RC4 berdasarkan Avalanche Effect.
4. Mengetahui pengaruh dari perbedaan resolusi citra dan panjang karakter yang dimasukkan terhadap kecepatan waktu eksekusi.

### 1.4 Batasan Masalah

Untuk mendapatkan hasil yang spesifik sesuai dengan yang diinginkan, dalam penelitian kali ini ditentukan batasan masalah sebagai berikut:

1. Data yang akan di enkripsi berupa teks bisa di input langsung maupun dari file berekstensi (.txt);
2. Citra yang akan digunakan sebagai citra sisipan merupakan citra digital berjenis *true color* (RGB);
3. Tidak Mencakup aspek pengamanan pada saat proses pengiriman citra stego.

4. Perangkat lunak yang dibangun hanya dapat dijalankan pada perangkat berbasis Android.

## **1.5 Sistematika Penulisan**

Sistematika penulisan tugas akhir ini mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya, antara lain:

### **BAB I. PENDAHULUAN**

Pada bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan.

### **BAB II. KAJIAN LITERATUR**

Pada bab ini membahas dasar-dasar teori yang akan digunakan pada penelitian ini, mulai dari tahapan analisis, perancangan, dan implementasi.

### **BAB III. METODOLOGI PENELITIAN**

Pada bab ini akan dilakukan pembahasan mengenai tahapan apa saja yang akan dilakukan pada penelitian ini. Masing-masing dari rencana tahapan penelitian dideskripsikan dengan rinci dan mengacu pada kerangka kerja. Pada akhir bab akan dipaparkan rancangan manajemen proyek pada pelaksanaan penelitian.

## **1.6 Kesimpulan**

Pada bab ini telah diberikan penjelasan umum mengenai penelitian yang akan dilakukan, meliputi latar belakang, rumusan masalah, tujuan, manfaat penelitian, batasan masalah dan sistematika penulisan.

## DAFTAR PUSTAKA

- A.S, Rosa. & Shalahuddin, M. 2013. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Jakarta: Informatika.
- Akash, Bath Kumar, M. & Rana, P. 2018. An Improved Method of Steganography Combined with Cryptography. *International Journal of Advance Engineering and Research Development*, 5(3): 434–439.
- AL-Shaaby, A.A. & AlKharobi, T. 2017. Cryptography and Steganography: New Approach. *Transactions on Networks and Communications*, 5(6).
- Anshori, Y., Dodu, A.Y.E. & Purwaningsih, M. 2019. SATIN – Sains dan Teknologi Informasi Aplikasi Steganografi pada Media Citra Digital Menggunakan Metode Least Significant Bit ( LSB ). 5(1): 1–10.
- Atee, H.A., Ahmad, R. & Noor, N.M. 2014. Combining Cryptography and Steganography for Data Hiding in Images. *conference of Applied Computer and Applied Computational Science (ACACOS)*, (April 2014): 128–134.
- Mukhtar, H 2018. *Kriptografi Untuk Keamanan Data*. Yogyakarta: Deepublish.
- Kroll, P. & Kruchten, P. 2003. *The Rational Unified Process Made Easy*. Rational Unified Process Made Easy: A Practitioner’s Guide to the RUP.
- Ricky, M., Setyaningsih, F.A. & Dipenogoro, M. 2018. Analisis Kompresi Steganography Pada Citra Digital Dengan Menggunakan Metode Least Significant Bit Berbasis Mobile. 06(03): 75–86.
- Kamble, B.H & Meshram B.B. 2012. Robustness of RC4 against Differential attack. *International Journal of Advanced Research in Computer Engineering & Technology*, 1(4): 661-665.

- Singhal, N. & Raina, J.P.S. 2011. Comparative Analysis of AES and RC4 Algorithms for Better Utilization. *International Journal of Computer Trends and Technology*, (July to Aug): 177–181.
- Sumartono, I., Putera, A., Siahaan, U. & Mayasari, N. 2016. An Overview of the RC4 Algorithm. *IOSR Journal of Computer Engineering*, 18(6): 67–73.
- Djuwitaningrum, E.R. & Apriyani, M. 2016. Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit Dan Algoritma LsCG. *Juita*, IV(2): 79–85.
- Yandala, Melvin. 2019. Steganografi Citra Berwarna Terenkripsi dengan Skema Kriptografi Visual Hou di dalam Media Citra dengan Metode Least Significant Bit.
- Septyaningtyas, V., Niken, C. & Mulyana, A. 2014. Analisis Algoritma RC4 Sebagai Metode Enkripsi WPA-PSK Pada Sistem Keamanan Jaringan Wireless LAN. *e-Proceeding of Engineering*, 1(1), 28-35.
- Zhou, X., Gong, W., Fu, W. & Jin, L. 2016. An improved method for LSB based on color image steganography combined with cryptography. *IEEE/ACIS 15th International Conference of Computer and Information Science, ICIS 2016 - Proceedings*, 4–7.
- Anggreni, N.A.S., Linawati. & Sastra, I.N.P. Sistem Pengamanan Anonym dengan Menggunakan Kriptografi ElGamal. *Majalah Ilmiah Teknologi Elektro*, 18(2): 197-202.