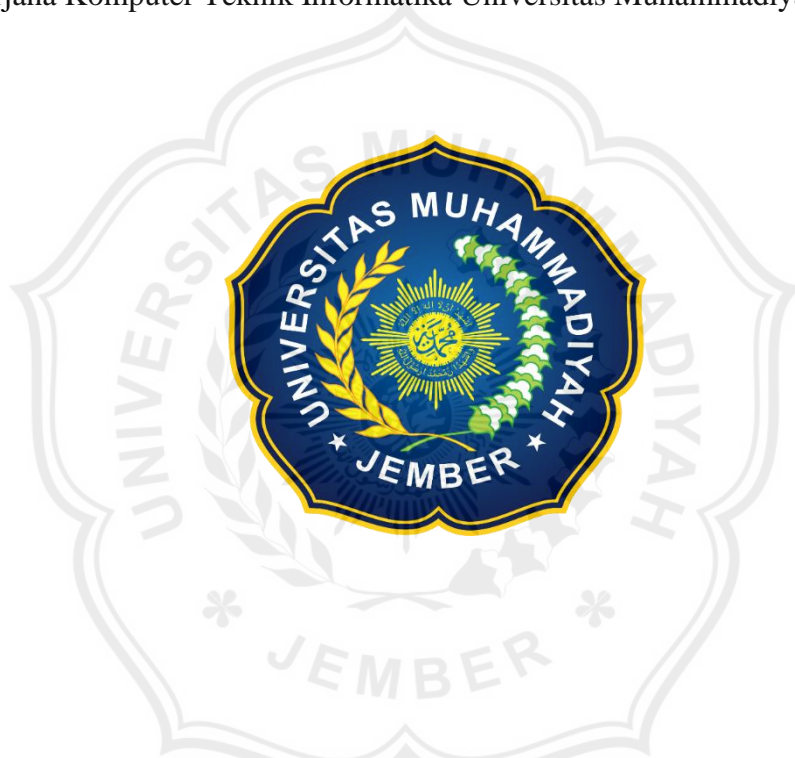


TUGAS AKHIR

IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RSA DENGAN ALGORITMA STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB) SEBAGAI WATERMARKING UNTUK PELABELAN IDENTITAS PADA FILE CITRA DIGITAL

Disusun Untuk melengkapi dan Memenuhi Syarat Kelulusan Guna Meraih Gelar
Sarjana Komputer Teknik Informatika Universitas Muhammadiyah Jember



Dimas Wahyu Nurdiansyah

15 1065 1132

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2020

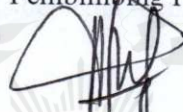
HALAMAN PENGESAHAN

**IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RSA
DENGAN ALGORITMA STEGANOGRAFI LEAST SIGNIFICANT
BIT(LSB) SEBAGAI WATERMARKING UNTUK PELABELAN
IDENTITAS PADA FILE CITRA DIGITAL**

DIMAS WAHYU NURDIANSYAH
1510651132

Telah Mempertanggung Jawabkan Laporan Tugas Akhirnya
Pada Sidang Tugas Akhir Tanggal 31 Januari 2020
Sebagai Salah Satu Syarat Kelulusan
Guna Meraih Gelar Sarjana Komputer
Program Studi Teknik Informatika Universitas Muhammadiyah Jember

Disetujui Oleh :
Dosen pembimbing :
Pembimbing I



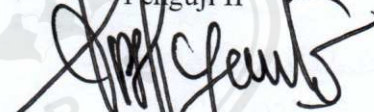
Triawan Adi Cahyanto, M.Kom
NPK. 12 03 719

Dosen penguji :
Penguji I



Agung Nilogiri, S.T., M.Kom
NIP. 19770330 200501 1 002

Dosen Penguji :
Penguji II



Deni Arifianto, M.Kom
NPK. 11 03 588

Mengesahkan,
Dekan Fakultas Teknik



Ir. Suhartinah, M.T
NPK. 95 05 246

Mengetahui,
Ketua Program Studi Teknik Informatika



Triawan Adi Cahyanto, M.Kom
NPK. 12 03 719

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : DIMAS WAHYU NURDIANSYAH

NIM : 1510651132

INSTITUSI : Strata-1 Program Studi Teknik Informatika Fakultas Teknik,
Universitas Muhammadiyah Jember

Menyatakan bahwa Tugas Akhir yang berjudul **“Implementasi Algoritma Kriptografi Kunci Publik RSA Dengan Algoritma Steganografi Least Significant Bit (LSB) Sebagai Watermarking Untuk Pelabelan Identitas Pada File Citra Digital”** bukan merupakan Tugas Akhir orang lain baik sebagian maupun keseluruhan kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya dan apabila pernyataan ini tidak benar penulis bersedia mendapatkan sanksi dari akademik.

Jember, 31 Januari 2020

Yang menyatakan,



DIMAS WAHYU N.

NIM. 1510651132

UNGKAPAN TERIMAKASIH

Alhamdulillah puji syukur kepada Allah swt, karena kehendak dan ridhaNya, peneliti dapat menyelesaikan tugas akhir ini. Peneliti sadari tugas akhir ini tidak akan selesai tanpa doa, dukungan dan dorongan dari berbagai pihak.

Atas segala upaya, bimbingan, dan arahan dari semua pihak tanpa mengurangi rasa hormat, penulis mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Ibu Ir. Suhartinah, M.T selaku dekan Fakultas Teknik Universitas Muhammadiyah Jember.
2. Bapak Triawan Adi Cahyanto, M.Kom. selaku Ketua Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember, dan juga sebagai dosen pembimbing utama laporan tugas akhir yang telah memberikan bimbingan serta pengarahan sehingga tugas akhir ini dapat terselesaikan..
3. Bapak Agung Nilogiri, S.T., M.Kom. selaku dosen penguji 1 yang telah memberikan kritik dan saran yang membangun dalam penelitian ini.
4. Bapak Deni Arifianto, M.Kom. selaku dosen penguji 2 yang telah memberikan kritik dan saran yang membangun dalam penelitian ini.
5. Orang tua dan segenap keluarga besarku yang telah banyak mendukung dan memberikan doanya dalam penyusunan laporan tugas akhir ini.
6. Teman sekaligus mentor matlab mas Agus Wirayasa.
7. Teman-teman “mbulet” yang juga ikut membantu dan memberi semangat yaitu Bagas (wifi gratis), Adon (teman ghibah), Yogi (teman ngopi), Dwi (fans one piece), Gigih (anak gamer), Tante Firda (mantanya Yogi), Bude Sintia (sang army).

Penulis menyadari bahwa dalam penyusunan laporan ini masih banyak kekurangan, oleh karena itu kritik dan saran yang bersifat membangun akan sangat berguna kearah kesempurnaan dan semoga tugas akhir ini dapat berguna bagi rekan-rekan mahasiswa fakultas teknik pada khususnya teknik informatika dan pembaca pada umumnya.

MOTTO

Tindakan kebaikan terkecil bernilai lebih dari niat terbesar.

(Kahlil Gibran)

Tidak masalah selambat apapun kamu bergerak, asalkan jangan berhenti.

(Confucius)

Kesehatanmu lebih penting dari skripsimu, jadi berliburlah jika lelah.

(Dimas Wahyu Nurdiansyah)



KATA PENGANTAR

Puji syukur kehadiran Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul “Implementasi Algoritma Kriptografi Kunci Publik RSA dengan Algoritma Steganografi Least Significant Bit (LSB) sebagai Watermarking untuk Pelabelan Identitas pada File Citra Digital”. Tugas akhir ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan pendidikan Strata Satu (S1) pada jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember.

Penyusunan tugas akhir ini tidak lepas dari bantuan berbagai pihak. Oleh karena ini penulis menyampaikan terimakasih kepada :

1. Triawan Adi Cahyanto, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember dan juga dosen pembimbing utama.
2. Agung Nilogiri, S.T., M.Kom. selaku dosen penguji I dan Deni Arifianto, M.Kom. selaku dosen penguji II, yang telah meluangkan waktu, tenaga, pikiran, dan perhatian dalam penulisan skripsi ini.
3. Dosen dan karyawan Fakultas Teknik Universitas Muhammadiyah Jember.
4. Semua pihak yang tidak bisa disebutkan satu persatu.

Dengan segala kerendahan hati, penulis memohon maaf jika ternyata di kemudian hari diketahui bahwa hasil dari proyek akhir ini masih jauh dari kesempurnaan. Semoga bermanfaat bagi setiap insan yang mempergunakannya untuk kebaikan di jalan Allah SWT.

Jember, 31 Januari 2020

Penulis

DAFTAR ISI

| | |
|---|-------|
| HALAMAN SAMPUL..... | i |
| HALAMAN JUDUL | ii |
| HALAMAN PENGESAHAN | iii |
| HALAMAN PERNYATAAN..... | iv |
| UNGKAPAN TERIMA KASIH | v |
| MOTTO | vi |
| KATA PENGANTAR..... | vii |
| ABSTRAK | viii |
| ABSTRACT | ix |
| DAFTAR ISI..... | x |
| DAFTAR GAMBAR..... | xixii |
| DAFTAR TABEL | xiii |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah..... | 3 |
| 1.3 Batasan Masalah..... | 3 |
| 1.4 Tujuan Penelitian | 4 |
| 1.5 Manfaat Penelitian | 4 |
| BAB II TINJAUAN PUSTAKA | |
| 2.1 Kriptografi | 5 |
| 2.1.1 Definisi Kriptografi..... | 5 |
| 2.1.2 Konsep Kriptografi | 5 |
| 2.1.3 Tujuan Kriptografi | 6 |
| 2.1.4 Jenis Kriptografi | 7 |
| 2.1.5 Landasan Matematika Kriptografi | 9 |
| 2.2 Steganografi | 10 |
| 2.2.1 Definisi Kriptografi..... | 10 |
| 2.2.2 Konsep Kriptografi | 10 |
| 2.3 Watermarking | 11 |
| 2.4 Citra Digital | 12 |
| 2.4.1 Definisi Citra Digital..... | 12 |
| 2.4.2 Jenis Citra Digital | 13 |

| | | |
|--|---|-----------|
| 2.5 | Rivest-Shamir-Adleman | 15 |
| 2.5.1 | Algoritma RSA Pembangkit Pasangan Kunci..... | 15 |
| 2.5.2 | Algoritma Enkripsi RSA | 15 |
| 2.5.2 | Algoritma Dekripsi RSA..... | 16 |
| 2.6 | Least Sifnificant Bit..... | 16 |
| 2.6.1 | Algoritma Embedding Least Significant Bit..... | 17 |
| 2.6.2 | Algoritma Extraction Least Significant Bit | 17 |
| 2.7 | MATLAB | 18 |
| 2.8 | MSE dan PSNR | 18 |
| BAB III METODOLOGI PENELITIAN | | |
| 3.1 | Tahapan Penelitian..... | 21 |
| 3.2 | Analisa Kebutuhan Sistem | 21 |
| 3.2.1 | Kebutuhan Fungsional | 22 |
| 3.2.2 | Kebutuhan Non Fungsional | 22 |
| 3.3 | Analisa Pemodelan Sistem | 23 |
| 3.3.1 | Flowchart Sistem..... | 24 |
| 3.3.2 | Contoh Perhitungan..... | 25 |
| 3.4 | Pengujian..... | 28 |
| BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEEM | | |
| 4.1 | Kebutuhan Perangkat Lunak dan Perangkat Keras | 29 |
| 4.2 | Implementasi..... | 29 |
| 4.2.1 | Enkripsi dan Embedding | 30 |
| 4.2.2 | Extraction dan Dekripsi | 31 |
| 4.2.3 | Histogram RGB..... | 32 |
| 4.2.4 | MSE dan PSNR..... | 33 |
| 4.3 | Analisis Dalam Aplikasi..... | 33 |
| 4.4 | Hasil Pengujian Sistem | 43 |
| BAB V KESIMPULAN DAN SARAN | | |
| 5.1 | Kesimpulan | 59 |
| 5.2 | Saran..... | 60 |
| DAFTAR PUSTAKA..... | | 61 |
| LAMPIRAN..... | | 62 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2.1 Skema Enkripsi dan Dekripsi Pesan..... | 6 |
| Gambar 2.2 Skema Kriptografi Simetris..... | 7 |
| Gambar 2.3 Skema Kriptografi Asimetris..... | 8 |
| Gambar 2.4 Skema Penyisipan dan Ekstraksi Pesan | 11 |
| Gambar 2.5 Matriks Citra Digital..... | 12 |
| Gambar 2.6 Contoh Citra Biner | 13 |
| Gambar 2.7 Gradasi Citra Grayscale | 13 |
| Gambar 2.8 Contoh Citra Grayscale | 13 |
| Gambar 2.9 Contoh Citra RGB..... | 14 |
| Gambar 2.10 Tampilan Awal Matlab | 18 |
| Gambar 2.11 Rumus Mean Square Error | 19 |
| Gambar 2.12 Rumus Peak Signal to Noise Ratio | 19 |
| Gambar 3.1 Skema Alur Penelitian..... | 20 |
| Gambar 3.2 Diagram Blok Sistem RSA dan LSB | 22 |
| Gambar 3.3 Flowchart Penyisipan dan Enkripsi Label Citra Digital | 23 |
| Gambar 3.4 Flowchart Ekstraksi dan Dekripsi Label Citra Digital..... | 24 |
| Gambar 4.1 Halaman Utama | 28 |
| Gambar 4.2 Form Enkripsi dan Embedding..... | 29 |
| Gambar 4.3 Form Extraction dan Dekripsi | 30 |
| Gambar 4.4 Tampilan Menu Histogram RGB..... | 31 |
| Gambar 4.5 Tampilan Menu MSE dan PSNR | 32 |
| Gambar 4.6 Gambar Penampung(.png) | 33 |
| Gambar 4.7 Citra Stego yang sudah terkandung label (.png) | 40 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 3.3.1 Pencarian Nilai d | 25 |
| Tabel 4.3.1 Pencarian Nilai d | 34 |
| Tabel 4.3.2 Plaintext rubah ke ASCII | 34 |
| Tabel 4.3.3 Hasil Ciphertext dari Proses Enkripsi | 35 |
| Tabel 4.3.4 Hasil Convert Ciphertext ke Biner..... | 36 |
| Tabel 4.3.5 Nilai RGB channel Red..... | 37 |
| Tabel 4.3.6 Nilai RGB channel Green | 38 |
| Tabel 4.3.7 Nilai RGB channel Blue | 39 |
| Table 4.4.1 Citra Pengujian | 42 |
| Table 4.4.2 Pengujian Fungsional Citra 1 | 43 |
| Tabel 4.4.3 Pengujian Waktu Proses dan Panjang Karakter | 49 |
| Tabel 4.4.4 Hasil Pengujian Penyisipan dengan variasi Cover Image..... | 50 |
| Tabel 4.4.5 Hasil Manipulasi Stego Image pada citra 3 | 51 |
| Tabel 4.4.6 Hasil Histogram RGB citra 1 | 53 |
| Tabel 4.4.7 Nilai PSNR..... | 55 |
| Tabel 4.4.8 Nilai MSE dan PSNR..... | 55 |

