



### **Hak cipta dan penggunaan kembali:**

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

### **Copyright and reuse:**

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

**IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN  
STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK  
PENYIMPANAN IDENTITAS**

**SKRIPSI**

**Diajukan sebagai salah satu syarat untuk memperoleh gelar  
Sarjana Komputer (S.Kom.)**



**Christofer Derian Budianto**

**14110110019**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN INFORMATIKA  
UNIVERSITAS MULTIMEDIA NUSANTARA  
TANGERANG  
2018**

**LEMBAR PENGESAHAN SKRIPSI**  
**IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN**  
**STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK**  
**PENYIMPANAN IDENTITAS**

Oleh

Nama : Christofer Derian Budianto  
NIM : 14110110019  
Fakultas : Teknik dan Informatika  
Program Studi : Informatika

Tangerang, 9 Mei 2018

Ketua Sidang



Ni Made Satvika Iswafi, S.T., M.T.

Dosen Penguji



Dennis Gunawan, S.Kom., M.Sc.

Dosen Pembimbing I



Arya Wicaksana, S.Kom., M.Eng.Sc.,

Dosen Pembimbing II



Seng Hansun, S.Si., M.Cs.

OCA, CEH

Mengetahui,

Ketua Program Studi

Informatika



Seng Hansun, S.Si., M.Cs.

## PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya,

Nama : Christofer Derian Budiarto

NIM : 14110110019

Fakultas : Teknik dan Informatika

Program Studi : Informatika

menyatakan bahwa skripsi yang berjudul **“IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS”** ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan / penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 9 Mei 2018



(Christofer Derian Budiarto)

**PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK  
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Christofer Derian Budianto

NIM : 14110110019

Program Studi : Informatika

Fakultas : Teknik dan Informatika

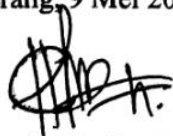
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui dan memberikan izin kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalti-Free Right*) atas karya ilmiah saya yang berjudul: **Implementasi Kriptografi Kurva Eliptik dan Steganografi Least Significant Bit untuk Penyimpanan Identitas** beserta perangkat yang diperlukan.

Dampak Hak Bebas Royalti Non-eksklusif ini, pihak Universitas Multimedia Nusantara Berhak menyimpan, mengalihmedia atau *format*-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mendistribusi dan menampilkan atau mempublikasikan karya ilmiah saya di internet atau media lain untuk kepentingan akademis, tanpa perlu meminta izin dari saya maupun memberikan royalti kepada saya, selama tetap mencantumkan nama saya sebagai penulis karya ilmiah tersebut.

Demikian pernyataan ini saya buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Tangerang, 9 Mei 2018



(Christofer Derian Budianto)

## KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa, karena hanya dengan berkat dan rahmat-Nya lah, skripsi dengan judul **“IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK PENYIMPANAN IDENTITAS”** ini dapat diselesaikan. Penulisan skripsi ini merupakan syarat kelulusan pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.

Atas bimbingan, dan saran yang telah diberikan selama proses penulisan skripsi, ucapan terimakasih disampaikan kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, Ph.D., selaku Dekan Fakultas Teknik dan Informatika,
3. Seng Hansun, S.Si., M.Cs., selaku Ketua Program Studi dan dosen pembimbing dalam penyusunan skripsi, yang telah membimbing dan membagi ilmunya selama penulisan skripsi,
4. Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, CEH, selaku dosen pembimbing dalam penyusunan skripsi, yang telah membimbing dan membagi ilmunya selama penulisan skripsi,
5. Ayah, ibu, dan seluruh keluarga yang selalu mendoakan dan memberi dukungan moral dari awal hingga akhir penulisan skripsi,
6. Febrian Wilson, Nathania Elvina, Rakadetyo Alif, Kevin Alexander, Willy William, dan Keshia Tiffany yang telah membantu dalam penyelesaian skripsi, baik secara langsung maupun tidak,

7. Ang Rahma, Indah Novia, Enrico Nathaniel, Janssen, Ferdinand, Yudha Teguh Hartanto, Kenny Wantara, Albert Kosasi, Astrid Tamara, Marisa Tri Utami, Tri Nita, Klara Livia, Nesa Alicia, Yosua Winata, Monique Subandi, Viktor, Vicky Reynaldo, Cynthia Sinly dan Gisela Felicia yang telah memberikan bantuan dan dukungan moral selama pengerjaan skripsi,
8. Teman-teman Laboratorium B507 yang telah membantu dalam pengerjaan skripsi,
9. Teman-teman di Program Studi Informatika Universitas Multimedia Nusantara, yang telah menjadi rekan belajar dan berdiskusi selama perkuliahan di Universitas Multimedia Nusantara, dan
10. Seluruh pihak lain yang tidak dapat disebutkan satu per satu, yang telah membantu, mendukung, memberi semangat dalam penulisan skripsi.

Semoga skripsi ini dapat memberikan manfaat bagi para pembaca.

Tangerang, 9 Mei 2018

Christofer Derian Budianto

UMMN  
UNIVERSITAS  
MULTIMEDIA  
NUSANTARA

**IMPLEMENTASI KRIPTOGRAFI KURVA ELIPTIK DAN  
STEGANOGRAFI LEAST SIGNIFICANT BIT UNTUK  
PENYIMPANAN IDENTITAS  
ABSTRAK**

Pencurian identitas merupakan masalah keamanan yang serius. Kerugian yang ditimbulkan akibat pencurian identitas tidak hanya berupa kerugian materiil namun juga kerugian non materiil seperti kerugian sosial. Di Indonesia, identitas yang resmi diakui di seluruh Negara Kesatuan Republik Indonesia, adalah Kartu Tanda Penduduk (KTP) Indonesia. Untuk mengamankan identitas tersebut dapat digunakan metode kriptografi dan steganografi sehingga identitas terlindungi oleh dua lapisan keamanan. Kriptografi merupakan teknik untuk mengubah suatu informasi menjadi samar agar tidak mudah dipahami oleh orang lain. Kriptografi kurva eliptik merupakan algoritma kriptografi kunci publik yang memanfaatkan kurva elips matematis. Steganografi merupakan teknik untuk menyembunyikan data agar keberadaannya tidak diketahui oleh orang lain. Steganografi *least significant bit* merupakan algoritma untuk menyembunyikan data pada *least significant bit* dari suatu citra digital. Pengujian menunjukkan bahwa *cipher text* yang dihasilkan selalu dua kali lebih panjang dari *plain text*. Hasil rata-rata PSNR yang dihasilkan sebesar 64.97. Nilai tersebut menunjukkan bahwa hasil keluaran aplikasi memiliki tingkat kemiripan yang tinggi.

Kata Kunci: identitas, kriptografi, kriptografi kurva eliptik, *least significant bit*, steganografi





# **IMPLEMENTATION OF ELLIPTICAL CURVE CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT STEGANOGRAPHY FOR SECURING**

**IDENTITY**

**ABSTRACT**

Identity theft is one of the most serious security threats. Identity theft could cause not only financial loss but also social loss. Indonesia officially recognizes Kartu Tanda Penduduk (KTP) as the legal identity card for its citizens. In order to keep the identity secure, cryptography and steganography used to provide two layers of protection. Cryptography is a technique to change an information into a secret, so as not easily understood by others. Elliptical curve cryptography is a cryptography that uses mathematical elliptic curve. Steganography is a technique to hide data so that its existence is not known by others. Least significant bit steganography is an algorithm that hides data in the least significant bit of a file. The implementation and testing show that the proposed methods are successful for securing identity. The length of cipher text is twice of the plain text. The average PSNR value obtained from the implementation of LSB method is 64.97. The result show that the output is acceptable in terms of security of the ECC and also obscurity of the LSB.

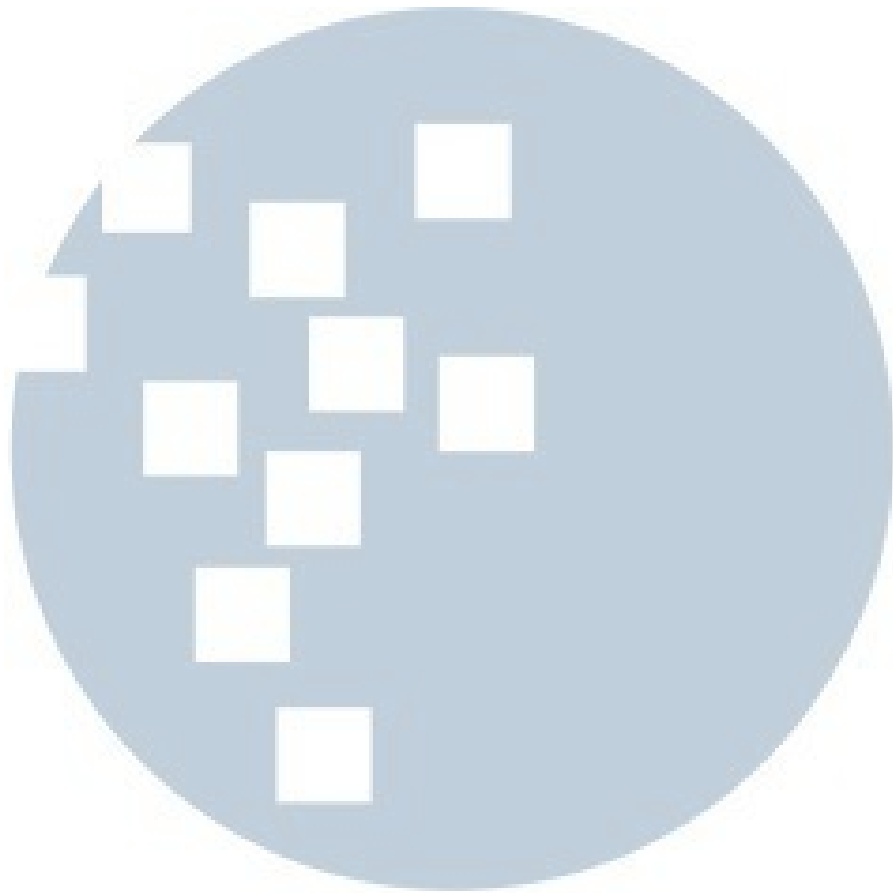
Keywords: cryptography, elliptical curve cryptography, identity, least significant bit, steganography

**UMN**

**UNIVERSITAS  
MULTIMEDIA  
NUSANTARA**

## DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI .....	<b>Error! Bookmark not defined.</b>
PERNYATAAN TIDAK MELAKUKAN PLAGIAT .....	<b>Error! Bookmark not defined.</b>
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS .....	<b>Error! Bookmark not defined.</b>
KATA PENGANTAR .....	iv
ABSTRAK .....	vii
ABSTRACT .....	viii
DAFTAR RUMUS .....	x
DAFTAR GAMBAR .....	xi
DAFTAR TABEL .....	xii
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang Masalah .....	1
1.2 Rumusan Masalah .....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	4
1.5 Manfaat Penelitian .....	5
1.6 Sistematika Penulisan Laporan Penelitian .....	5
BAB II LANDASAN TEORI .....	7
2.1 Identitas .....	7
2.2 Pencurian Identitas .....	8
2.3 Kriptografi .....	10
2.3.1 Kriptografi Kurva Eliptik .....	11
2.4 Steganografi .....	16
2.4.1 Least Significant Bit .....	17
2.4.2 Peak Signal to Noise Ratio .....	19
2.5 Portable Network Graphics .....	20
2.6 Uji Korelasi .....	21
BAB III METODOLOGI DAN PERANCANGAN APLIKASI .....	23
3.1 Metodologi Penelitian .....	23
3.2 Flowchart .....	24
3.3 Rancangan Tampilan Antarmuka .....	36
BAB IV IMPLEMENTASI DAN UJI COBA .....	40
4.1 Spesifikasi Perangkat .....	40
4.2 Implementasi Aplikasi .....	40
4.3 Pengujian dan Evaluasi .....	46
4.3.1 Pengujian Implementasi Algoritma Kriptografi Kurva Eliptik .....	46
4.3.2 Pengujian Implementasi Algoritma Least Significant Bit .....	65
4.3.3 Evaluasi Hasil .....	73
BAB V KESIMPULAN DAN SARAN .....	81
5.1 Kesimpulan .....	81
5.2 Saran .....	81
DAFTAR PUSTAKA .....	83
DAFTAR LAMPIRAN .....	87



UMMN

UNIVERSITAS  
MULTIMEDIA  
NUSANTARA

## DAFTAR RUMUS

Rumus 2.1 Syarat Pertidaksamaan Variabel $a, b$ .....	12
Rumus 2.2 <i>Quadratic Residue Module</i> .....	12
Rumus 2.3 Persamaan Kurva Eliptik .....	13
Rumus 2.4 Persamaan Titik $x$ pada Penjumlahan Titik .....	15
Rumus 2.5 Persamaan Titik $y$ pada Penjumlahan Titik .....	15
Rumus 2.6 Persamaan Titik $x$ pada Penggandaan Titik.....	15
Rumus 2.7 Persamaan Titik $y$ pada Penggandaan Titik.....	15
Rumus 2.8 Persamaan Enkripsi untuk $c_1$ .....	16
Rumus 2.9 Persamaan Enkripsi untuk $c_2$ .....	16
Rumus 2.10 Persamaan Dekripsi .....	16
Rumus 2.11 <i>Mean Square Error</i> .....	19
Rumus 2.12 <i>Peak Signal to Noise Ratio</i> .....	19
Rumus 2.13 Uji Korelasi .....	22

UMMN

UNIVERSITAS  
MULTIMEDIA  
NUSANTARA

## DAFTAR GAMBAR

Gambar 2.1 <i>Field</i> pada Kartu Tanda Penduduk (KTP) Indonesia .....	9
Gambar 2.2 <i>Identity Theft Model</i> .....	9
Gambar 2.3 Kurva Eliptik untuk $a=4, b=9$ .....	12
Gambar 2.4 Sebaran titik pada kurva dengan $a = 4, b = 9, \text{ dan } p = 13$ .....	14
Gambar 2.5 Contoh 3 <i>pixel</i> dari Gambar 24-bit color .....	18
Gambar 2.6 Hasil Penyisipan Karakter "A" .....	18
Gambar 3.1 <i>Flowchart</i> Aplikasi.....	25
Gambar 3.2 <i>Flowchart</i> Simpan Identitas .....	26
Gambar 3.3 Proses Inisialisasi Kurva .....	27
Gambar 3.4 Proses Enkripsi .....	28
Gambar 3.5 Proses Steganografi .....	30
Gambar 3.6 <i>Flowchart</i> Ambil Identitas .....	32
Gambar 3.7 <i>Flowchart</i> Ekstrak Teks .....	33
Gambar 3.8 Proses <i>Reverse Bit</i> .....	34
Gambar 3.9 Proses Dekripsi.....	35
Gambar 3.10 Halaman Awal Aplikasi .....	36
Gambar 3.11 Rancangan Halaman Simpan Identitas.....	37
Gambar 3.12 Rancangan Halaman <i>Upload</i> Gambar.....	37
Gambar 3.13 Rancangan <i>Upload Stego Image</i> .....	38
Gambar 3.14 Rancangan Halaman Lihat Identitas .....	38
Gambar 3.15 Rancangan Halaman Cara Pemakaian.....	39
Gambar 3.16 Rancangan Halaman <i>Credits</i> .....	39
Gambar 4.1 Halaman Utama Aplikasi .....	41
Gambar 4.2 Halaman Simpan Identitas .....	42
Gambar 4.3 Halaman <i>Upload</i> Gambar.....	43
Gambar 4.4 Halaman <i>Upload Stego Image</i> .....	44
Gambar 4.5 Halaman Lihat Identitas .....	44
Gambar 4.6 Halaman <i>Credits</i> .....	45
Gambar 4.7 Halaman Cara Pemakaian .....	45
Gambar 4.8 <i>Code</i> Proses Enkripsi .....	53
Gambar 4.9 <i>Code</i> Proses Dekripsi .....	63
Gambar 4.10 <i>Code</i> Mengosongkan Bit Terakhir .....	66
Gambar 4.11 <i>Code</i> Penyisipan ke Bit Terakhir .....	66
Gambar 4.12 <i>Code</i> Pengambilan Bit Terakhir .....	68
Gambar 4.13 <i>Code Reverse</i> Susunan Bit .....	69
Gambar 4.14 Contoh Hasil Aplikasi PSNR 1.2.....	71
Gambar 4.15 Kurva Eliptik untuk $a = 6, b = 7$ .....	73
Gambar 4.16 Sebaran Titik untuk $a = 6, b = 7, p = 61$ .....	73
Gambar 4.17 Kurva Eliptik untuk $a = 7, b = 8$ .....	74
Gambar 4.18 Sebaran Titik untuk $a = 7, b = 8, p = 67$ .....	74
Gambar 4.19 Kurva Eliptik untuk $a = 40, b = 33$ .....	75
Gambar 4.20 Sebaran Titik untuk $a = 40, b = 33, p = 71$ .....	75
Gambar 4.21 Lena.....	79

## DAFTAR TABEL

Tabel 2.1 Tabel Domain Parameter .....	12
Tabel 2.2 Hasil Quadratic Residue Module .....	13
Tabel 2.3 Hasil Persamaan Kurva Eliptik .....	13
Tabel 2.4 Perbandingan Format Gambar .....	21
Tabel 4.1 Karakter dalam Penelitian .....	46
Tabel 4.2 Nilai Variabel untuk Tiga Skenario .....	47
Tabel 4.3 Data Skenario 1 .....	49
Tabel 4.4 Data Skenario 2 .....	50
Tabel 4.5 Data Skenario 3 .....	51
Tabel 4.6 Kunci Publik .....	52
Tabel 4.7 Kunci Privat .....	53
Tabel 4.8 Hasil Skenario 1, Data 1 .....	58
Tabel 4.9 Hasil Skenario 1, Data 2 .....	59
Tabel 4.10 Hasil Skenario 1, Data 3 .....	59
Tabel 4.11 Hasil Skenario 1, Data 4 .....	59
Tabel 4.12 Hasil Skenario 2, Data 1 .....	60
Tabel 4.13 Hasil Skenario 2, Data 2 .....	60
Tabel 4.14 Hasil Skenario 2, Data 3 .....	60
Tabel 4.15 Hasil Skenario 2, Data 4 .....	61
Tabel 4.16 Hasil Skenario 3, Data 1 .....	61
Tabel 4.17 Hasil Skenario 3, Data 2 .....	61
Tabel 4.18 Hasil Skenario 3, Data 3 .....	62
Tabel 4.19 Hasil Skenario 3, Data 4 .....	62
Tabel 4.20 Perbandingan Panjang <i>Plain</i> dan <i>Cipher Text</i> .....	62
Tabel 4.21 Perbandingan Cover Image dan Stego Image .....	71
Tabel 4.22 Data Parameter Kurva Penelitian .....	76
Tabel 4.23 Data Uji Korelasi Sebaran Titik Maksimal .....	76
Tabel 4.24 Nilai PSNR pada Gambar Lena .....	79
Tabel 4.25 Data <i>Cipher</i> dengan PSNR .....	79

U I V N  
U N I V E R S I T A S  
M U L T I M E D I A  
N U S A N T A R A