

# **PENYEMBUNYIAN DATA RAHASIA DALAM GAMBAR MENGUNAKAN PENDEKATAN *PREDICTIVE CODING***

Disusun Oleh :

**Nama : Dedy Santosa**

**Nrp : 0422167**

Jurusan Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha,  
Jl. Prof.Drg.Suria Sumantri, MPH no.65, Bandung, Indonesia.

**Email : dedy\_zainal@yahoo.com**

## **ABSTRAK**

Steganografi merupakan ilmu dan seni yang mempelajari teknik dan cara penyembunyian pesan rahasia di dalam suatu media sedemikian rupa sehingga pihak ke-tiga tidak dapat melihat dan menyadari keberadaan pesan rahasia dalam media tersebut.

Pada Tugas Akhir ini, algoritma steganografi dibentuk menggunakan pendekatan *predictive coding* yang merupakan bagian dari proses kompresi. *Predictive coding* adalah proses prediksi yang dilakukan oleh sebuah *predictor* untuk memprediksi setiap nilai *pixel host-image* sehingga menghasilkan *predictive pixel value* (PPV). Tiga *predictor* yang digunakan adalah *median edge detection* (MED), *modified median edge detection* (MMED) dan *gradient adjusted prediction* (GAP). Bit data rahasia hasil dari proses enkripsi, secara berurutan akan disisipkan pada setiap *error value* (EV) dengan bantuan *operator* modula. Nilai EV yang dimaksud adalah beda antara *original pixel value* (OPV) pada *host-image* dan PPV yang diperoleh dari *predictor*. Diharapkan kombinasi antara steganografi dan enkripsi ini mampu meningkatkan keamanan data rahasia.

Dari hasil uji coba, diperoleh bahwa data rahasia dapat disembunyikan dalam citra dan dikembalikan ke bentuk semula tanpa kesalahan dengan menggunakan pendekatan *predictive coding*. Berdasarkan nilai PSNR dan MOS dari *stego-image*, diperoleh *predictor* yang paling baik digunakan adalah *predictor* MMED yang diikuti secara berurutan oleh *predictor* MED dan GAP.

Kata kunci : Steganografi, *Predictive Coding*, MED, MMED, GAP

# **HIDING SECRET DATA IN IMAGE USING PREDICTIVE CODING APPROACH**

Composed by :

**Name : Dedy Santosa**

**Nrp : 0422167**

Departement Of Electrical Engineering, Faculty Of Engineering, Maranatha  
Christian University,

Jl. Prof.Drg.Suria Sumantri, MPH no.65, Bandung, Indonesia.

**Email : dedy\_zainal@yahoo.com**

## **ABSTRACT**

Steganography is the science and art of studying the techniques and ways of hiding a secret message in a medium such that third parties can't see and realize the existence of secret messages in the media.

In this final project, steganography algorithm is formed using predictive coding approach that is part of the compression process. Predictive coding is a prediction process which is done by a predictor to predict each pixel value of host-image that resulting predictive pixel value (PPV). Three predictors that are used in this final project are median edge detection (MED), modified median edge detection (MMED) and the gradient adjusted prediction (GAP). Bits of secret data that resulted from encryption process will be inserted sequentially on each error value (EV) with Modula operator assistance. The EV value is the difference between the original pixel value (OPV) of the host-image and PPV obtained from the predictor. It is expected that the combination of steganography and encryption is able to increase the security of confidential data.

The test results show that the confidential data can be hidden in the image and restored to its original shape without error by using predictive coding approach. Based on PSNR and MOS values of the stego-image, the best predictor is MMED predictor followed by the MED and GAP predictors respectively.

Keyword : *Steganography, Predictive Coding, MED, MED, GAP*

## DAFTAR ISI

	Halaman
ABSTRAK .....	i
ABSTRACT.....	ii
DAFTAR ISI.....	iii
DAFTAR TABEL.....	v
DAFTAR GAMBAR .....	vii
DAFTAR LAMPIRAN.....	ix
BAB I PENDAHULUAN	
I.1 Latar Belakang .....	1
I.2 Identifikasi Masalah .....	2
I.3 Perumusan Masalah .....	2
I.4 Tujuan Tugas Akhir .....	2
I.5 Pembatasan Masalah .....	2
I.6 Sistematika Penulisan .....	3
BAB II LANDASAN TEORI	
II.1 Kriptografi .....	5
II.2 Steganografi .....	6
II.3 AES ( <i>Advanced Encryption Standar</i> ).....	9
II.4 <i>Predictive Coding</i> .....	13
II.4.1 <i>Predictor MED</i> dan <i>MMED</i> .....	14
II.4.2 <i>Predictor GAP</i> .....	16
II.5 <i>Huffman Coding</i> .....	18
II.5.1 <i>Huffman Encoding</i> .....	18
II.5.2 <i>Huffman Decoding</i> .....	21
II.6 <i>MOS (Mean Opinion Score)</i> .....	22
II.7 <i>PSNR (Peak Signal to Noise Ratio)</i> .....	22
II.8 Matlab 7.0 .....	23

II.9 <i>Graphical User Interface</i> (GUI).....	24
BAB III PERANCANGAN DAN REALISASI	
III.1 Diagram Sistem Penyembunyian Data Rahasia.....	26
III.1.1 Prosedur Penyembunyian .....	26
III.1.2 Prosedur Ekstraksi .....	28
III.2 Perancangan dan Realisasi Sistem Penyembunyian Data Rahasia ....	28
III.2.1 Perancangan <i>Graphical User Interface</i> (GUI) .....	28
III.2.2 Realisasi <i>Graphical User Interface</i> (GUI) .....	30
III.2.3 Realisasi Algoritma AES-128 .....	30
III.2.3.1 Realisasi Prosedur Enkripsi AES-128 .....	32
III.2.3.2 Realisasi Prosedur Dekripsi AES-128.....	33
III.2.4 Realisasi Sistem PREDICT .....	33
III.2.4.1 Realisasi <i>Predictor</i> MED dan MMED .....	36
III.2.4.2 Realisasi <i>Predictor</i> GAP .....	37
III.2.5 Realisasi Penyisipan Bit Data Rahasia .....	40
III.2.6 Realisasi Ekstraksi Bit Data rahasia .....	41
BAB IV ANALISA DAN DATA PENGAMATAN	
IV.1 Menghitung Nilai PSNR dan MOS.....	43
IV.1.1 Menghitung Nilai PSNR dan MOS <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak).....	52
IV.1.2 Menghitung Nilai PSNR dan MOS <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks) .....	57
IV.1.3 Menghitung Nilai PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Polos dan Data rahasia Berupa Teks).....	61
BAB V KESIMPULAN DAN SARAN	
V.1 Kesimpulan .....	65
V.2 Saran .....	65
DAFTAR PUSTAKA .....	66

## DAFTAR TABEL

	Halaman
Tabel 2.1 Jumlah Putaran Pengoperasian AES-128 .....	12
Tabel 2.2 Representasi Tiap Simbol Dari Pohon Huffman.....	19
Tabel 2.3 Skala Penilaian Subyektif .....	22
Tabel 4.1 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak) Menggunakan <i>Predictor</i> MED.....	55
Tabel 4.2 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak) Menggunakan <i>Predictor</i> GAP	56
Tabel 4.3 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak) Menggunakan <i>Predictor</i> MMED .....	56
Tabel 4.4 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 8.192 <i>byte</i> ) Menggunakan <i>Predictor</i> MED ( $h = 1$ ).....	58
Tabel 4.5 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 8.192 <i>byte</i> ) Menggunakan <i>Predictor</i> GAP ( $h = 1$ ).....	58
Tabel 4.6 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 8.192 <i>byte</i> ) Menggunakan <i>Predictor</i> MMED ( $h = 1$ ) .....	58
Tabel 4.7 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 16.384 <i>byte</i> ) Menggunakan <i>Predictor</i> MED ( $h = 2$ ).....	59
Tabel 4.8 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 16.384 <i>byte</i> ) Menggunakan <i>Predictor</i> GAP ( $h = 2$ ).....	59

Tabel 4.9 Nilai MOS dan PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Bercorak dan Data Rahasia Berupa Teks Rahasia 16.384 <i>byte</i> ) Menggunakan <i>Predictor</i> MMED ( $h = 2$ ) .....	60
Tabel 4.10 Jumlah Kesalahan Data Rahasia .....	61
Tabel 4.11 Nilai PSNR <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Abu-abu Polos dan Data Rahasia Berupa Teks Rahasia 8.192 <i>byte</i> ( $h = 1$ ) dan 16.384 <i>byte</i> ( $h = 2$ )).....	64

## DAFTAR GAMBAR

	Halaman
Gambar 2.1 Blok diagram Enkripsi AES .....	11
Gambar 2.2 Blok Diagram Dekripsi AES .....	13
Gambar 2.3 Pola Kausal <i>Predictor</i> MED dan MMED.....	14
Gambar 2.4 Dua Contoh Deteksi Tepi pada <i>Predictor</i> MED .....	15
Gambar 2.5 Pola Kausal <i>Predictor</i> GAP .....	16
Gambar 2.6 Contoh Deteksi Tepi Menggunakan <i>Predictor</i> GAP.....	17
Gambar 2.7 Langkah Pembentukan Pohon Huffman .....	20
Gambar 3.1 Blok Diagram Sistem Penyembunyian Data Rahasia.....	27
Gambar 3.2 Blok Diagram GUI STG.....	29
Gambar 3.3 Blok Diagram GUI RECEIV .....	29
Gambar 3.4 Diagram Alir Utama Pemograman Penyambunyian Data Rahasia.....	31
Gambar 3.5 Diagram Alir Utama Pemograman Ekstraksi .....	32
Gambar 3.6 Diagram Alir Prosedur Enkripsi AES-128 .....	34
Gambar 3.7 Diagram Alir Prosedur Dekripsi AES-128.....	35
Gambar 3.8 Diagram Alir Sistem PREDICT .....	36
Gambar 3.9 Blok Diagram <i>Predictor</i> MED .....	37
Gambar 3.10 Blok Diagram <i>Predictor</i> MMED.....	37
Gambar 3.11 Diagram Alir <i>Predictor</i> MED dan MMED.....	38
Gambar 3.12 Diagram Alir <i>Predictor</i> GAP .....	39
Gambar 3.13 Diagram Alir Fungsi Embedncompress .....	41
Gambar 3.14 Diagram Alir Fungsi Receiver_.....	42
Gambar 4.1 Citra Asli (256 x 256 <i>pixel</i> ) .....	44
Gambar 4.2 Citra Rahasia (128x64 <i>pixel</i> ) .....	45
Gambar 4.3 Langkah Pertama (Menampilkan GUI STG).....	45
Gambar 4.4 Langkah ke-dua (Memasukkan Nama <i>File Host-Image</i> ) .....	46
Gambar 4.5 Langkah ke-tiga (Melakukan Proses Prediksi pada <i>Host-Image</i> Menggunakan <i>Predictor</i> MED).....	46

Gambar 4.6 Hasil Proses Prediksi .....	47
Gambar 4.7 Langkah ke-empat (Memasukkan Nama <i>File</i> Data Rahasia dan Menentukan Jumlah Bit Per <i>Pixel</i> penyisipan).....	47
Gambar 4.8 Langkah ke-lima (Melakukan Proses Enkripsi) .....	48
Gambar 4.9 Hasil Proses Enkripsi.....	48
Gambar 4.10 Langkah ke-enam (Melakukan Proses Penyisipan).....	49
Gambar 4.11 Hasil Proses Penyembunyian) .....	49
Gambar 4.12 Langkah pertama (Menampilkan GUI RECEIV).....	50
Gambar 4.13 Langkah ke-dua (Memasukkan Nama <i>File Stego-Image</i> Terkompresi) .....	50
Gambar 4.14 Langkah ke-tiga (Melakukan Prosedur Ekstraksi) .....	51
Gambar 4.15 Hasil Proses Ekstraksi .....	51
Gambar 4.16 <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak) .....	54
Gambar 4.17 Citra Rahasia Hasil Ekstraksi <i>Stego-Image</i> ( <i>Host-Image</i> dan Data Rahasia Berupa Citra Bercorak) .....	55
Gambar 4.18 <i>Stego-Image</i> ( <i>Host-Image</i> Berupa Citra Abu-abu Polos dan Data Rahasia Berupa Teks Rahasia 8.192 <i>byte</i> ( $h = 1$ ) dan 16.384 <i>byte</i> ( $h = 2$ )) .....	63



## DAFTAR LAMPIRAN

	Halaman
LAMPIRAN A ALGORITMA AES-128 .....	A-1
LAMPIRAN B DATA PENGAMATAN HASIL PERCOBAAN .....	B-1