

## DESAIN DAN IMPLEMENTASI STEGANALISIS CITRA DIGITAL MENGGUNAKAN METODE KLASIFIKASI JARINGAN SARAF TIRUAN PADA ANDROID MINI PC

Dhion Azrya Dewangga<sup>1</sup>, Dr. Bambang Hidayat <sup>2</sup>, Sugondo Hadiyoso<sup>3</sup>

<sup>1</sup>Teknik Elektro, Fakultas Teknik Elektro, Universitas Telkom

---

### Abstrak

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia, sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi digital menggunakan media digital sebagai media penyembunyian, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Untuk mengetahui ada atau tidaknya pesan rahasia dalam suatu media, dibutuhkan steganalisis.

Pada tugas akhir ini dilakukan implementasi steganalisis citra digital pada Android Mini PC. Sebelum dilakukan klasifikasi, terlebih dahulu dilakukan pre-processing untuk mempermudah proses steganalisis. Setelah dilakukan pre-processing, dilakukan proses identifikasi ciri menggunakan data statistik citra, seperti mean, variance, skewness, dan kurtosis, dalam domain DWT. Kemudian dilakukan klasifikasi dengan Jaringan Saraf Tiruan (JST) metode pembelajaran backpropagation untuk menentukan ada atau tidaknya suatu pesan tersembunyi dalam citra digital tersebut.

Hasil yang didapatkan dalam penyelesaian tugas akhir ini yaitu terimplementasikannya sebuah program pada Android Mini PC yang dapat mengklasifikasikan ada atau tidaknya suatu pesan rahasia yang disembunyikan dalam citra digital dengan menggunakan Jaringan Saraf Tiruan. Tingkat akurasi yang didapatkan mencapai 66.7% dengan waktu komputasi rata-rata 3.16 detik.

Kata Kunci : steganalisis, citra digital, Jaringan Saraf Tiruan, dan Android Mini PC.

---

### Abstract

Steganography is the science and art of hiding secret message, so that the existence of the message is not detected by human senses. Digital steganography uses digital media as cover, such as image, sound, text, and video. Hidden secret data can also be image, sound, text, or video. To determine whether or not the secret message in the media, it needs steganalysis.

In this final project, it is implemented digital image steganalysis on Android Mini PC. Before classifying, first pre-processing image to simplify the process. After pre-processing, the identification process is carried out using the statistical characteristics, such as mean, variance, skewness, and kurtosis of the image in DWT domain. Then the classification is performed by backpropagation Artificial Neural Network (ANN) for determining whether or not there is a hidden message in a digital image.

The results obtained in this final project is a program on Android Mini PC that can classify whether or not there is a secret message hidden in a digital image using Artificial Neural Network. The level of accuracy obtained is up to 66.7%, while the average processing time is 3.16 seconds.

Keywords : steganalysis, digital image, Artificial Neural Network, and Android Mini PC.

---

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi memberikan pengaruh besar bagi kehidupan manusia. Saat ini, banyak pesan diamankan dengan metode steganografi. Steganografi adalah ilmu dan seni menyembunyikan suatu informasi, sehingga keberadaan informasi tidak terdeteksi oleh indera manusia. Informasi berupa citra, audio, video ataupun teks dapat disembunyikan ke dalam media cover atau media penyembunyian berupa citra, audio, video ataupun teks juga. Hal ini memberi kesempatan yang luas untuk komunikasi rahasia. Akibatnya, metode untuk mendeteksi komunikasi rahasia diperlukan. Tugas ini sangat mendesak untuk penegakan hukum, misalnya untuk badan-badan intelijen dalam mencegat komunikasi musuh.

Steganalisis merupakan suatu teknik untuk mendeteksi pesan tersembunyi yang disembunyikan menggunakan steganografi. Tujuan dari steganalisis adalah untuk mengidentifikasi apakah suatu media yang dicurigai mempunyai pesan tersembunyi atau tidak dan jika memungkinkan, mengekstraksi data tersembunyi. Steganalisis dikatakan berhasil apabila dapat mendeteksi adanya pesan. Dalam beberapa tahun terakhir, penelitian mengenai steganalisis banyak dilakukan, salah satunya adalah steganalisis menggunakan jaringan saraf tiruan [5], namun masih berupa simulasi.

Dari uraian di atas, pada penulisan tugas akhir ini dibahas bagaimana mengimplementasikan steganalisis pada Android Mini PC untuk mendeteksi ada atau tidaknya suatu pesan tersembunyi dalam suatu media, khususnya pada media citra digital. Pada citra digital dilakukan proses ekstraksi ciri untuk mendapatkan ciri-ciri statistik citra, berupa *mean*, *variance*, *skewness*, dan *kurtosis*, dalam domain wavelet. Domain wavelet dipilih karena ciri-ciri yang didapatkan pada domain ini lebih baik daripada ciri pada domain spasial ataupun kosinus. Korelasi setiap ciri pada subband yang sama bersifat *independent*, sehingga cocok untuk steganalisis [4]. Selain itu, perubahan citra menjadi citra stego dapat dikatakan sebagai penambahan noise. Perubahan-perubahan ini dapat dilihat dengan jelas

pada domain wavelet [1]. Setelah ciri didapatkan, digunakan klasifikasi jaringan saraf tiruan *backpropagation* untuk membedakan citra cover dan citra stego.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang, permasalahan yang diteliti dalam pembuatan tugas akhir ini di antaranya sebagai berikut.

1. Bagaimana menganalisis ada atau tidaknya pesan rahasia pada suatu citra digital menggunakan jaringan saraf tiruan.
2. Bagaimana implementasi steganalisis menggunakan klasifikasi jaringan saraf tiruan pada Android Mini PC.
3. Bagaimana kecepatan proses steganalisis pada Android Mini PC.
4. Berapa tingkat akurasi steganalisis.

## 1.3 Batasan Masalah

Batasan-batasan masalah yang ditetapkan, yaitu:

1. Steganalisis dilakukan pada citra digital *grayscale* berformat JPEG dengan ukuran 512x512 piksel.
2. Steganalisis bersifat pasif, yaitu hanya mendeteksi keberadaan steganografi.
3. Ekstraksi ciri pada citra dilakukan dalam domain DWT, dekomposisi wavelet menggunakan metode Haar.
4. Metode pengenalan pola pada jaringan saraf tiruan adalah metode *backpropagation*.
5. Proses steganografi menggunakan aplikasi yang sudah ada.
6. Tidak membahas mengenai proses steganografi.
7. Citra digital tidak memiliki noise.

## 1.4 Tujuan

Didasari rumusan masalah yang telah dijelaskan sebelumnya, tujuan yang dicapai dalam pengerjaan tugas akhir ini adalah:

1. Menganalisis ada atau tidaknya pesan rahasia pada suatu citra digital menggunakan jaringan saraf tiruan.

2. Mengimplementasikan steganalisis menggunakan klasifikasi jaringan saraf tiruan pada Android Mini PC.
3. Mengetahui kecepatan proses steganalisis pada Android Mini PC.
4. Mengetahui tingkat akurasi steganalisis.

## 1.5 Metodologi

Metodologi yang digunakan dalam melakukan pemecahan masalah di atas adalah metode eksperimen. Metode ini terdiri dari beberapa tahap, yaitu:

### 1. Studi Literatur

Mengumpulkan sejumlah literatur, materi, atau referensi ilmiah yang berkaitan dengan permasalahan steganalisis untuk mendukung pembentukan landasan teori dalam pengerjaan tugas akhir ini.

### 2. Analisis dan Perancangan Kebutuhan Sistem

Pada tahap ini dilakukan perancangan program serta pengumpulan sejumlah basis data dari citra digital yang akan digunakan dalam proses steganalisis.

### 3. Implementasi dan Pembuatan Sistem

Pada tahap ini direalisasikan rancangan sistem yang telah dibuat pada tahapan sebelumnya untuk menghasilkan sebuah program yang dapat melakukan steganalisis pada Android Mini PC.

### 4. Pengujian Sistem

Sistem yang dihasilkan kemudian diuji dengan menghitung waktu komputasi dan akurasi.

### 5. Analisis Hasil Pengujian

Dari hasil pengujian yang dilakukan pada tahapan sebelumnya, maka pada tahap ini dilakukan analisis terkait hasil pengujian yang dilakukan, juga meliputi kesimpulan dari hasil penelitian ini.

### 6. Penyusunan Laporan Tugas Akhir

Pada tahapan ini dilakukan penyusunan laporan tugas akhir ke dalam bentuk buku Tugas Akhir beserta pengumpulan beberapa dokumentasi yang diperlukan terkait referensi, proses, maupun hasil penelitian yang

dilakukan, dengan mengikuti kaidah penulisan yang benar dan sesuai dengan ketentuan-ketentuan yang telah ditetapkan.

## 1.6 Sistematika Penulisan

Penulisan tugas akhir dengan judul “Desain dan Implementasi Steganalisis Citra Digital Menggunakan Metode Klasifikasi Jaringan Saraf Tiruan pada Android Mini PC” ini memiliki sistematika penulisan sebagai berikut.

### BAB I PENDAHULUAN

Bab pendahuluan berisi latar belakang pembuatan tugas akhir, permasalahan yang dibahas, pembatasan masalah, tujuan, metodologi, dan sistematika penulisan tugas akhir.

### BAB II DASAR TEORI

Bab dasar teori membahas teori yang menjadi landasan atau pendukung dalam pembuatan tugas akhir, seperti citra digital, steganalisis, DWT, dan JST.

### BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab perancangan dan implementasi sistem menjelaskan proses desain, realisasi sistem, jenis-jenis serangan yang digunakan, dan parameter pengujian, termasuk diagram blok dan diagram alir sistem.

### BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab pengujian sistem dan analisis hasil membahas analisis hasil simulasi. Analisis dilakukan terhadap parameter kinerja sistem yang diamati.

### BAB V PENUTUP

Bab penutup berisi kesimpulan dari seluruh pembahasan yang dilakukan dan saran untuk memperbaiki tugas akhir ini.

## BAB V

### PENUTUP

#### 5.1 Kesimpulan

Berdasarkan pengujian yang dilakukan pada penelitian ini, dapat disimpulkan hal-hal sebagai berikut.

1. Sistem yang dibuat mampu melakukan proses steganalisis pada Android Mini PC.
2. Persentasi klasifikasi menggunakan jaringan saraf tiruan *backpropagation* untuk *seen images* yaitu 76.9% untuk *true positive*, 65.7% untuk *true negative*, 34.3% untuk *false positive*, dan 33.1% untuk *false negative*.
3. Persentasi klasifikasi menggunakan jaringan saraf tiruan *backpropagation* untuk *unseen images* yaitu 60% untuk *true positive*, 73.3% untuk *true negative*, 26.7% untuk *false positive*, dan 40% untuk *false negative*.
4. Berdasarkan *embedding rate* pesan rahasia disisipkan, citra stego dengan *embedding rate* 90% lebih mudah terdeteksi atau memiliki akurasi tertinggi, mencapai 60%. Semakin besar *embedding rate*, semakin mudah untuk mendeteksi citra stego.
5. Berdasarkan aplikasi steganografi yang digunakan, akurasi pendeteksian citra stego yang dihasilkan aplikasi SilentEye dan JPHide lebih besar dibandingkan citra stego OurSecret.
6. Proses steganalisis pada Android Mini PC berlangsung dengan cepat, rata-rata waktu yang dibutuhkan selama 3.16 detik, sehingga tidak membuat pengguna lama menunggu saat ingin memeriksa suatu citra.

#### 5.2 Saran

Penelitian lebih lanjut diharapkan dapat memperbaiki kekurangan yang ada. Untuk itu disarankan sebagai berikut.

1. Steganalisis dilakukan terhadap media lain, seperti audio dan video.

2. Steganalisis bersifat aktif, agar isi pesan dapat diketahui, tidak hanya mendeteksi keberadaan pesan.
3. Menambahkan step *embedding rate* steganografi dari 10% hingga 100% dengan rentang 10 agar dapat diketahui pada nilai *embedding rate* berapa aplikasi steganalisis dapat mendeteksi dengan benar.
4. Menggunakan dekomposisi paket wavelet pada citra agar lebih banyak bagian citra yang dianalisis sehingga akurasi dapat meningkat.
5. Pada proses ekstraksi ciri, digunakan ciri lain yang lebih mewakili citra agar tingkat akurasi yang didapatkan meningkat.
6. Menggunakan Android Mini PC dengan spesifikasi lebih baik atau mengimplementasikan di alat lainnya agar proses steganalisis menjadi lebih baik.



## DAFTAR PUSTAKA

- [1] Bhattacharyya, Souvik dan Gautam Sanyal. 2013. Moments and Similarity Measure Feature Based Image Steganalysis Technique (MSM). *International Journal of Information & Network Security (IJINS)*, Vol.2.
- [2] Brigida. 2012. *Jenis-jenis Citra Digital*. (Diakses di <http://informatika.web.id/jenis-jenis-citra-digital.htm> pada 25 Juni 2014.)
- [3] Chandramouli, Rajarathnam, dkk. 2004. *Image Steganography and Steganalysis: Concepts and Practice*. Springer-Verlag Berlin Heidelberg.
- [4] Chhikara, Rita dan Latika Singh. 2013. A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted. *International Journal of Engineering and Innovative Technology (IJEIT) Volume 3*.
- [5] Davidson, Jennifer, dkk. 2005. An Artificial Neural Network for Wavelet Steganalysis. *The International Society for Optical Engineering*, vol. 5916, *Mathematical Methods in Pattern and Image Analysis*.
- [6] Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta: Andi.
- [7] Gonzalez, R. C. 2002. *Digital Image Processing*. New Jersey: Prentice Hall.
- [8] Hermawan, Arief. 2006. *Jaringan Saraf Tiruan Teori dan Aplikasi*. Yogyakarta: Andi.
- [9] Krenn, J.R. 2004. *Steganography and Steganalysis*.
- [10] Munir, Rinaldi. 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung: Informatika.
- [11] Nugraha, Zulfi. 2013. *Desain dan Implementasi Optical Character Recognition Menggunakan Jaringan Syaraf Tiruan pada FPGA*. Bandung: Institut Teknologi Telkom.
- [12] Press, William H., dkk. 1992. *Numerical Recipes in C: The Art of Scientific Computing*. New York: Cambridge University Press.
- [13] Raniprima, Sevierda. 2014. *Simulasi dan Analisis Steganografi Citra Digital dengan Enkripsi Berdasarkan Prinsip Kubus Rubik*. Bandung: Universitas Telkom.

- [14] Rikomagic. *Dual Core Mini PC MK802 III S*. (Diakses di [http://www.rikomagic.com/en/product/showpro\\_id\\_32\\_pid\\_19.html](http://www.rikomagic.com/en/product/showpro_id_32_pid_19.html) pada 9 September 2014.)
- [15] Safaat, Nazruddin. 2012. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung: Informatika.
- [16] Siang, Jok Jek. 2006. *Jaringan Syaraf Tiruan dan Pemrogramannya Menggunakan Matlab*. Yogyakarta: Andi.
- [17] Smartstat. 2010. *Ukuran Penyebaran (Measures of Dispersion)*. (Diakses di <http://smartstat.wordpress.com/2010/03/27/ukuran-penyebaran-measures-dispersion/> pada 10 September 2014.)
- [18] Walker, James S. 1999. *A Primer on Wavelets and Their Scientific Applications*. CRC Press.
- [19] [linux01.gwdg.de/~alatham/stego.html](http://linux01.gwdg.de/~alatham/stego.html)
- [20] [www.securekit.net/oursecret.htm](http://www.securekit.net/oursecret.htm)
- [21] [www.silenteye.org](http://www.silenteye.org)