IMPLEMENTASI STEGANALISIS DENGAN MENGGUNAKAN METODE BSM-SVM PADA STEGANOGRAFI CITRA DIGITAL

Anindito Setya Nugraha[1], Deni Saepudin[2], Adiwijaya[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Steganografi atau teknik penyisipan data saat ini sering sekali digunakan oleh banyak pihak untuk berbagai kepentingan, salah satunya adalah untuk penyelundupan data. Oleh karena itu diperlukan suatu aplikasi yang dapat mendeteksi teknik steganografi tersebut sehingga diharapkan mampu meminimalisir upaya penyelundupan data rahasia.

Steganalisis merupakan suatu disiplin ilmu yang mempelajari cara mendeteksi keberadaan teknik steganografi dalam suatu media tertentu. Salah satu teknik steganalisis ini adalah Binary Similarity Measures – Support Vector Machine (BSM-SVM) yang digunakan untuk mencari pola-pola tertentu pada suatu media pada level binary. Metode ini termasuk ke dalam metode blind steganalysis dimana metode ini mampu mendeteksi semua metode Steganografi dan pada semua format file dengan akurasi yang tinggi.

Pada tugas akhir diimplementasikan metode BSM-SVM untuk melakukan steganalisis terhadap beberapa set citra digital dengan tujuan apakah metode ini bisa mendeteksi teknik steganografi LSB dan F5 pada format BMP dan JPG. Berdasarkan pengujian yang telah dilakukan terhadap citra digital, Algoritma BSM-SVM mampu mendeteksi metode LSB dan F5 dan memiliki nilai akurasi yang mencapai 77,28% untuk deteksi metode LSB dan 76,49% untuk deteksi metode F5. Metode ini juga mampu diterapkan pada format citra digital berupa JPG dan BMP dimana pada JPG akurasinya mencapai 77,02% dan pada BMP sebesar 76,75%.

Kata Kunci :

Abstract

Nowadays, with little help from technology we can embed secret message into any digital media. Steganography is one of the technique that can be used to embed secret message into digital media. Sometimes these Steganography technique is used to do some illegal sharing activity. An application that is capable of detect this kind of secret message, are required in many cases. This application can be used to prevent the secret message from being spread publicly.

Steganalysis is a science techniques used for detecting any steganographic message in any digital media. One of the steganalysis method is Binary Similarity Measures - Support Vector Machine. This method is classified as a blind steganalysis technique which means able to detect all steganography technique with high accuracy.

Based on the testing result, the Binary Similarity Measures - Support Vector Machine algorithm has an accuracy value reaching up to 77,28% for detecting LSB method and 76,49% for detecting F5 method. This steganalysis technique also can be used for various digital image format like JPG and BMP. The accuracy for JPG is 77,02% and for BMP is 76,75%. And more bigger the embedded message filesize it will be easier for this technique to detect the message.

Keywords : Image, Steganography, Steganalysis, Binary Similarity Measures, Support Vector Machine.

---

1. Pendahuluan

1.1 Latar Belakang

Steganografi merupakan salah satu teknik untuk menyisipkan pesan rahasia di dalam suatu media, teknik ini semakin berkembang dewasa ini. Dalam perkembangannya, data rahasia dapat disembunyikan pada media digital seperti citra, audio dan video[8]. Sayangnya tidak semua penggunanya menggunakan teknik steganografi untuk tujuan baik bahkan teknik ini sering kali dimanfaatkan beberapa pihak yang tidak bertanggung jawab untuk menyelundupkan data. Salah satu contohnya adalah data perusahaan yang sering diselundupkan oleh pegawai perusahaan tersebut ke berbagai pihak. Secara visual media digital biasa dan stego-objek pada teknik steganografi ini tidak dapat dibedakan secara kasat mata, sehinga kita tidak menyadari bahwa di dalam suatu data digital terdapat pesan rahasia. Oleh karena itu diperlukan suatu cara untuk mengawasi data digital yang kita anggap penting.

Steganalisis merupakan suatu teknik untuk mengetahui apakah di dalam suatu objek terdapat pesan yang telah disisipkan menggunakan steganografi atau tidak[3]. Kabar baiknya adalah menurut Avcibas[1] dari semua teknik steganografi ini terdapat pola-pola tertentu pada stego-objek yang memungkinkan untuk di deteksi dengan pendekatan tersendiri. Bentuk pendekatan yang ditawarkan adalah penggunaan Binary Similarity Measures – Support Vector Machine (BSM-SVM) untuk mendeteksi perubahan pada level biner. Metode Binary Similarity Measure – Support Vector Machine ini dipilih dikarenakan termasuk metode universal atau blind steganalisis yang artinya mampu mendeteksi semua jenis steganografi.

Dalam tugas akhir ini penulis mencoba melakukan implementasi dan analisis metode BSM-SVM (*Binary Similarity Measures-Support Vector Machine*) untuk mendeteksi steganografi yang paling umum digunakan dan paling sederhana yaitu metode LSB (*Least Significant Bit*)[15] dan metode steganografi yang memiliki ketahanan tinggi terhadap serangan visual maupun statistik yaitu F5[6]. Diharapkan nantinya penelitian ini dapat mengimplementasikan metode BSM-SVM sebagai metode steganalisis dalam mendeteksi perbedaan antara stego-objek dengan media digital biasa sehingga bisa mencegah terjadinya penyusupan data melalui teknik steganografi.

1.2 Perumusan Masalah

Pada penelitian Tugas Akhir ini, penelitian difokuskan pada analisis dan implementasi steganalisis citra *digital* menggunakan algoritma *Binary Similarity Measures – Support Vector Machine*. Berdasarkan latar belakang masalah, maka beberapa permasalahan utama yang akan dirumuskan antara lain:

a. Bagaimana menerapkan teknik steganalisis untuk mendeteksi adanya objek steganografi dalam sebuah media digital.
b. Bagaimana menerapkan teknik binary similarity measure untuk meng-ekstrak nilai statistik dari suatu media digital.
c. Bagaimana pembuatan klasifikasi dengan memanfaatkan support vector machine untuk membedakan kelas citra digital dengan objek steganografi dan kelas citra digital kosong.

1.3 Batasan Masalah

Yang menjadi batasan masalah dalam tugas akhir ini adalah :

a. File yang disisipkan pada Stego-Objek berbentuk text.
b. Objek atau file host yang digunakan untuk menyisipkan file berupa citra digital berformat BMP dan JPG.
c. Metode yang digunakan pada steganografi adalah Least Significant Bit(LSB) dan F5.

1.4 Tujuan

Tujuan yang ingin dicapai dalam pengerjaan Tugas Akhir ini adalah sebagai berikut:

a. Mengimplementasikan steganalisis untuk mendeteksi adanya objek steganografi dalam suatu citra digital.
b. Menganalisis performansi sistem dengan melihat nilai akurasi-nya.

1.5 Hipotesis

Penggunaan BSM-SVM sebagai metode steganalisis dapat mendeteksi steganografi LSB dan F5 pada format JPG dan BMP.

1.6 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan untuk penyelesaian permasalahan diatas adalah dengan menggunakan langkah-langkah sebagai berikut :

1. Studi literatur

   Pada tahap ini dilakukan pencarian sumber-sumber bacaan atau referensi dari buku, artikel maupun paper-paper yang terdapat pada internet serta memahami dan mempelajarinya sehingga dapat digunakan sebagai dasar teori dalam penyusunan Tugas Akhir ini. Literatur yang dicari adalah yang terkait dengan algoritma *BSM*, steganalisis, steganografi citra *digital* , serta informasi lain yang menunjang pembuatan tugas akhir ini.
2. Perancangan program yang akan dibuat.

   Pada tahap ini dilakukan perancangan perangkat lunak dalam membangun aplikasi desktop yang dapat melakukan steganalisis menggunakan algoritma *Binary Similarity Measures – Support Vector Machine*.
3. Implementasi

   Mengimplementasikan perancangan dengan menggunakan diagram alir (*flowchart)* yang telah dibuat untuk membangun aplikasi ini menggunakan java.
4. Pengujian dan analisa hasil

   Menganalisis hasil pengujian untuk mengetahui sejauh mana tingkat detection rate dari sistem yang telah dibangun.
5. Penarikan kesimpulan dan penyusunan laporan tugas akhir

   Tahap ini merupakan tahap penarikan kesimpulan terhadap pengujian yang telah dilakukan dan pembuatan laporan.

1.7 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan menggunakan sistematika sebagai berikut:

1. BAB 1

   Membahas mengenai latar belakang yang melandasi pengerjaan tugas akhir ini, rumusan masalah, batasan masalah, tujuan, serta metode penyelesaian masalah.
2. BAB 2

   Berisi tentang teori-teori yang mendukung di dalam pengerjaan tugas akhir ini.
3. BAB 3

   Berisi tentang proses perancangan sistem dan parameter-parameter yang akan diuji dan dianalisis.

4. BAB 4

   Berisi tentang implementasi baik di dalam perangkat keras maupun perangkat lunak, skenario yang dibuat untuk simulasi, serta pengujian dan analisis terhadap sistem yang telah dibangun.

5. BAB 5

   Berisi kesimpulan dari hasil analisis yang telah dilakukan dan saran-saran yang dapat digunakan untuk penelitian selanjutnya.

5. Penutup

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis pada penelitian tugas akhir ini, diperoleh beberapa kesimpulan sebagai berikut :

1. Semakin besar file yang disisipkan ke citra digital maka semakin besar beda nilai binary similarity measure dibandingkan dengan nilai binary similarity measure awal sehingga semakin besar file yang disisipkan semakin mudah di deteksi.
2. Metode binary similarity measure ini bisa diterapkan pada citra digital dengan format jpg dan bmp. Terbukti dari perbedaan nilai binary similarity measure yang sangat kecil pada citra digital berformat bmp dan jpg.
3. Proses klasifikasi pada studi kasus steganografi ini memiliki tingkat akurasi yang lebih tinggi ketika diklasifikasi menggunakan kernel Radial Basis Function(RBF) dibandingkan dengan linear kernel.
4. Dengan menggunakan metode *Binary similarity measure* didapat hasil akurasi yaitu 77,28% terhadap steganografi Least Significant Bit dan 76,49% untuk steganografi F5.

5.2 Saran

Adapun saran yang dapat diberikan, antara lain :

1. Penelitian dapat dikembangkan menggunakan media lain, seperti video, audio ataupun webpage.
2. Penelitian dapat dikembangkan dengan menguji metode steganografi lain seperti farid[10] dan lsb+.

Daftar Pustaka

[1] Avcibas, Ismail.Kharrazi, Mehdi.Memon, Nasir.Sankur,Bulent (2005). Images Steganalysis with Binary Similarity Measures. EURASIP Journal on Applied Signal Processing 2005, 2749-2757.

[2] Hsu, Wei C., Chang, Chung C., Lin, Jen C., (2010). A Practical Guide to Support Vector Classification. Dept. Of Computer Science and Information Engineering, NTU, Taiwan.

[3] Kharrazi, Mehdi., Sencar, Husrev T., Memon, Nasir. (2006). Improving Steganalysis by Fusion Techniques; A Case Study with Citra Steganography. Springer Berlin Heidelberg.

[4] Images were obtained from: philip.greenspun.com

[5] Da-Chun Wu, Wen-Hsiang Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Volume 24, Issues 9–10, June 2003

[6] Westfeld, Andreas. F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis. *Information Hiding*. Proceedings, LNCS 2137, Springer-Verlag Berlin 2001

[7] Fridrich, J.; Goljan, M.; Rui Du, "Detecting LSB steganography in color, and gray-scale images," *MultiMedia, IEEE* , vol.8, no.4, pp.22,28, Oct-Dec 2001

[8] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi "Steganografi dan Watermarking". Institut Teknologi Bandung.

[9] R. Chandramouli, M. Kharrazi, and N. Memon, Image Steganography and Steganalysis: Concepts and Practice, IWDW 2003, Korea.

[10] H. Farid, Detecting Hidden Messages Using Higher-Order Statistical Models, International Conference on Image Processing (ICIP), Rochester, NY, 2002

[11] Sutoyo, T,dkk. 2009, Teori Pengolahan Citra Digital, Penerbit Andi:Yogyakarta

[12] I. Bauermann and E. Steinbacj. Further Lossless Compression of JPEG Images. Proc. of Picture Coding Symposium (PCS 2004), San Francisco, USA, December 15–17, 2004.

[13] James D. Foley (1995). *Computer Graphics: Principles and Practice*. Addison-Wesley Professional.

[14] Vapnik, V. "The Nature of Statistical Learning Theory." *Data mining and knowledge discovery* (6): 1-47.

[15] Mitra, S., et al. "Steganalysis of LSB encoding in uncompressed images by close colour pair analysis." *IIT Kanpur Hacker's Workshop IITKHACK04*. 2004.