HASIL CEK_60020397_Point-C39-IRD-85Steganalisis Blind dengan Metode Convolutional Neural Network (CNN) Yedroudj-Net terhadap Tools Steganografi

by Imam Riadi 60020397

Submission date: 11-Dec-2020 10:22AM (UTC+0700)
Submission ID: 1471672879
File name: Neural_Network_CNN_Yedroudj-Net_terhadap_Tools_Steganografi.pdf (1.63M)
Word count: 5216
Character count: 32393

Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202073326
Vol. 7, No. 4, Agustus 2020, hlm. 787-796 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

STEGANALISIS *BLIND* DENGAN METODE CONVOLUTIONAL NEURAL NETWORK (CNN) YEDROUDJ-NET TERHADAP TOOLS STEGANOGRAFI

Nurmi Hidayasari*[1], Imam Riadi[2], Yudi Prayudi[3]

[1,3]Program Studi Teknik Informatika, Universitas Islam Indonesia Yogyakarta
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta
Email: [1]16917219@students.uii.ac.id, [2]imam.riadi@is.uad.ac.id, [3]prayudi@uii.ac.id
*Penulis Korespondensi

(Naskah masuk: 13 Maret 2020, diterima untuk diterbitkan: 21 April 2020)

Abstrak

Steganalisis digunakan untuk mendeteksi ada atau tidaknya file steganografi. Salah satu kategori steganalisis adalah blind steganalisis, yaitu cara untuk mendeteksi file rahasia tanpa mengetahui metode steganografi apa yang digunakan. Sebuah penelitian mengusulkan bahwa metode Convolutional Neural Networks (CNN) dapat mendeteksi file steganografi menggunakan metode terbaru dengan nilai probabilitas kesalahan rendah dibandingkan metode lain, yaitu CNN Yedroudj-net. Sebagai metode steganalisis Machine Learning terbaru, diperlukan eksperimen untuk mengetahui apakah Yedroudj-net dapat menjadi steganalisis untuk keluaran dari tools steganografi yang biasa digunakan. Mengetahui kinerja CNN Yedroudj-net sangat penting, untuk mengukur tingkat kemampuannya dalam hal steganalisis dari beberapa tools. Apalagi sejauh ini, kinerja Machine Learning masih diragukan dalam blind steganalisis. Ditambah beberapa penelitian sebelumnya hanya berfokus pada metode tertentu untuk membuktikan kinerja teknik yang diusulkan, termasuk Yedroudj-net. Penelitian ini akan menggunakan lima alat yang cukup baik dalam hal steganografi, yaitu Hide In Picture (HIP), OpenStego, SilentEye, Steg dan S-Tools, yang tidak diketahui secara pasti metode steganografi apa yang digunakan pada alat tersebut. Metode Yedroudj-net akan diimplementasikan dalam file steganografi dari output lima alat. Kemudian perbandingan dengan tools steganalisis lain, yaitu StegSpy. Hasil penelitian menunjukkan bahwa Yedroudj-net bisa mendeteksi keberadaan file steganografi. Namun, jika dibandingkan dengan StegSpy hasil gambar yang tidak terdeteksi lebih tinggi.

Kata kunci: Convolutional Neural Networks (CNN), blind steganalisis, steganalisis, CNN Yedroudj-net, tools steganografi.

BLIND STEGANALYSIS USING CONVOLUTIONAL NEURAL NETWORK YEDROUDJ-NET METHOD FOR STEGANOGRAPHY TOOLS

Abstract

Steganalysis is used to detect the presence or absence of steganograpy files. One category of steganalysis is blind steganalysis, which is a way to detect secret files without knowing what steganography method is used. A study proposes that the Convolutional Neural Networks (CNN) method can detect steganographic files using the latest method with a low error probability value compared to other methods, namely CNN Yedroudj-net. As the latest Machine Learning steganalysis method, an experiment is needed to find out whether Yedroudj-net can be a steganalysis for the output of commonly used steganography tools. Knowing the performance of CNN Yedroudj-net is very important, to measure the level of ability in terms of steganalysis from several tools. Especially so far, Machine Learning performance is still doubtful in blind steganalysis. Plus some previous research only focused on certain methods to prove the performance of the proposed technique, including Yedroudj-net. This research will use five tools that are good enough in terms of steganography, namely Hide In Picture (HIP), OpenStego, SilentEye, Steg and S-Tools, which is not known exactly what steganography methods are used on the tool. The Yedroudj-net method will be implemented in a steganographic file from the output of five tools. Then compare with other steganalysis tools, namely StegSpy. The results showed that Yedroudj-net could detect the presence of steganographic files. However, when compared with StegSpy the results of undetected images are higher.

Keywords: *Convolutional Neural Networks (CNN), blind steganalysis, steganalysis, CNN Yedroudj-net, tools steganography.*

1. PENDAHULUAN

Steganografi adalah teknik untuk menyembunyikan atau memasukkan pesan ke sebuah media, dapat berupa gambar, video, audio, dan lain-lain (Pipkorn and Weisbrot, 2012). Steganografi semakin mudah digunakan dengan tools gratis yang dapat dengan mudah ditemukan secara daring. Sebagian besar tools dirancang dengan teknik yang cukup aman, seperti penambahan kunci rahasia dan teknik enkripsi. Contoh alat steganografi adalah S-Tools, dan OpenStego.

Steganalisis sebagai metode anti-steganografi adalah teknik yang digunakan untuk mendeteksi keberadaan file steganografi. Steganalisis untuk tujuan yang baik dapat dijadikan tolak ukur untuk menemukan kelemahan, mengevaluasi serta mengembangkan metode steganografi.. Sehingga dapat meningkatkan teknik penyisipan yang lebih aman (Pamungkas, Hidayat and Andini, 2017). Sedangkan tujuan tidak baik, yaitu mencari celah dalam keberadaan pesan rahasia dan kemudian menghancurkannya.

Salah satu kategori utama steganalisis adalah steganalisis universal atau blind, yaitu steganalisis yang dilakukan tanpa mengetahui metode steganografi apa yang digunakan pada file. Blind steganalisis sulit diterapkan karena salah satu kendala yaitu sulitnya menemukan fitur yang relevan dengan karakteristik gambar steganografi. Kemudian, muncul machine learning yang digunakan untuk membuat model deteksi menggunakan data eksperimen (Karampidis, Kavallieratou and Papadourakis, 2018).

Salah satu contoh steganalisis menggunakan teknik *machine learning* adalah penelitian yang mengusulkan pendekatan *Stegography Pattern Discovery* (SPD). Dengan menggunakanaturan Fuzzy If-Then untuk mengekstrak identitas darisebuah gambar asli, yang terdiri dari dua tahap, yaitu tahap pertama menganalisa data set gambar untuk menemukan pola dari gambar stego. Kemudian kedua, alat steganalisis yang dibuat dilatih untuk mendeteksi satu metode steganografi khusus. Dengan metode ini tingkat deteksi meningkat dibandingkan dengan metode biasa lainnya. Rata-rata hasil akurasi yang diperoleh adalah 79–91% (Sajedi, 2016).

Steganalisis dengan teknik *machine learning* mulai berkembang. Beberapa tahun terakhir, *deep learning* menjadi alternatifyang menjanjikan untuk pendekatan steganalisis. Dengan pengetahuan utama tentang steganalisis gambar, yang menggabungkan fitur gambar yang lebih relevan dan prosedur klasifikasi terkini menggunakan*Convolutional Neural Networks* (CNN). Arsitektur CNN yang diusulkan tidak terlalu rumit, namun dengan filter yang jauh lebih banyak pada lapisan konvolusional akhir. Serta mampu menangani gambar yang lebih besar dan muatan yang lebih rendah.Steganalisis dengan teknik ini memperoleh hasil yang baik, dengan tingkat akurasi rata-rata 70-80% untuk penyisipan gambar dengan ukuran 0,1 bpp (bit per piksel) dan 90% untuk ukuran 0.4 bpp (Couchot et al., 2016).

Penelitian lain mengusulkan steganalisis berbasis CNN yang disebutkan mampu mendeteksi beberapa steganografi dengan metode terbaru dalam domain spasial untuk berbagai macam ukuran (0.05-0.5bpp) dan dengan nilai akurasi yang tinggi (Ye, Ni and Yi, 2017). Selanjutnya, CNN dikembangkan menjadi lebih kompleks dengan menambahkan jumlah filter yang digunakan pada masing-masing proses serta lima lapisan konvolusional dan *normalisasi batch*. Dengan nilai probabilitas eror-nya mencapai 14% (Yedroudj et al., 2018).

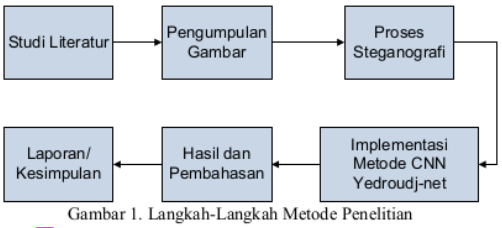
Sebagai salah satu metode steganalisis machine learning terbaru, diperlukan uji coba untuk mengetahui apakah CNN Yedroudj-net dapat menjadi steganalisis untuk output dari sejumlah tools yang biasa digunakan untuk steganografi. Mengetahui kinerja CNN Yedroudj-net pada beberapa tools steganografi sangat penting, untuk mengukur tingkat kemampuannya dalam hal steganalisis terhadap beberapa tools ini.

Terutama sejauh ini, kinerja machine learning masih diragukan pada blind steganalisis. Ditambah beberapa penelitian sebelumnya hanya berfokus pada metode tertentu untuk membuktikan kinerja metode yang diusulkan. Hingga saat ini, belum ada tinjauan komprehensif yang membahas kinerja steganalisis dengan pembelajaran mesin teknik terutama CNN Yedroudj-net sebagai steganalisis dari beberapa alat yang biasa digunakan di masyarakat. Oleh karena itu, dalam penelitian ini uji coba akan dilakukan pada CNN Yedroudj-net untuk menentukan sejauh mana kemampuannya mendeteksi steganografi yang dihasilkan dari tools.

Dalam penelitian ini akan menggunakan lima tools steganografi yang cukup baik, yaitu Hide In Picture (HIP), OpenStego, SilentEye, Steg dan S-Tools. Referensi (Hamid et al., 2013), menjelaskan bahwa OpenStego dan juga Hide In Picture termasuk tools yang memiliki kualitas yang baik berdasarkan hasil uji coba steganalisis dengan menghitung nilai PSNR (Peak Signal to Noise Ratio)-nya. Dalam hal ini PSNR digunakan untuk membandingkan kualitas media asli dan juga media steganografi. Pertimbangan lain menggunakan tools yang disebutkan sebelumnya adalah bahwa lima tools tersebut memiliki tingkat keamanan yang tinggi. Ini dapat dilihat oleh penulis secara langsung ketika menggunakan tools. Di mana setiap tools menyediakan fitur enkripsi pesan. Dengan penambahan teknik enkripsi, kemungkinan pesan akan semakin sulit dideteksi. Pertimbangan lain adalah bahwa kelima alat ini masih mudah ditemukan dan diunduh di situs online, sehingga siapa pun dapat menggunakannya secara bebas. Hal ini dapat menyebabkan penggunaan steganografi semakin meluas.

2. METODE PENELITIAN

Merupakan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah pada penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Langkah-Langkah Metode Penelitian

2.1 Studi Literatur

Studi literatur dilakukan untuk mendapatkan informasi serta referensi yang berhubungan dengan topik penelitian yang akan dilakukan, yang bersumber dari dokumen, buku, makalah, jurnal atau bahan tertulis lainnya. Baik berupa teori, laporan penelitian, atau penemuan sebelumnya, yang bersumber dari media daring maupun luring.
Studi literatur dilakukan terhadap penelitian-penelitian terkini yang terkait dengan steganografi dan juga steganalisis, serta metode-metode terbaru yang telah dikembangkan oleh peneliti lain dalam proses steganalisis. Dengan harapan dapat mendukung tujuan dari penelitian ini.

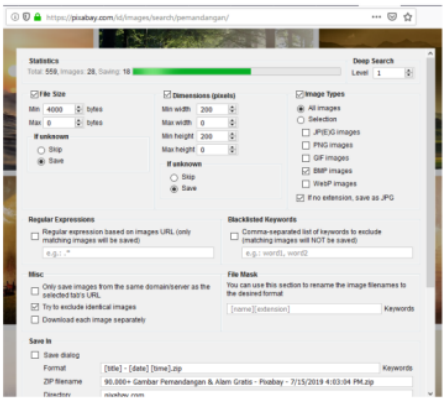
2.2 Pengumpulan Gambar

Tahap awal akan dilakukan pengumpulan gambar-gambar yang akan digunakan untuk menyembunyikan pesan. Gambar akan dikumpulkan atau diunduh dengan menggunakan bantuan Add-Ons DownThemAll yang disediakan oleh aplikasi peramban Firefox. Add-Ons tersebut dapat ditemukan di https://addons.mozilla.org/en-US/firefox/addon/save-all-images-webextension. Tampilannya dapat dilihat pada Gambar 2.

Proses penyimpanan gambar dengan menggunakan Add-Ons DownThemAll membutuhkan waktu yang tidak terlalu lama, tergantung dari banyak atau tidaknya gambar yang berhasil dikumpulkan.. Semua gambar secara otomatis disimpan dalam bentuk zip, sesuai dengan format yang tertera pada Add-Ons. Proses mengunduh gambar ini akan dilakukan beberapa kali sampai target gambar yang dibutuhkan terpenuhi.

2.3 Proses Steganografi dengan Tools

Selanjutnya adalah tahap melakukan proses steganografi dengan menggunakan lima *tools* yang telah disebutkan pada pendahuluan, yaitu Hide In Picture (HIP), OpenStego, SilentEye, Steg dan S-Tools. Tiap *tools* memiliki masukan dan keluaran dengan format gambar yang berbeda. Detailnya dapat dilihat pada Tabel 1.



Gambar 2. Tampilan Add-Ons DownThemAll

Tabel 1. Format Gambar yang Digunakan untuk Setiap Tools

Tools	Media Asli	Media Stego
HIP	BMP	BMP
OpenStego	JPG	PNG
Steg	JPG	JPG
S-Tools	BMP	BMP
SilentEye	BMP	BMP

2.3.1 Hide In Picture (HIP)

Hide In Picture (HIP), dibuat oleh Davi Tassinari de Figueireddo pada tahun 2001. Format yang dapat digunakan pada HIP adalah BMP dan GIF. Pada HIP, bit-bit file pesan akan disimpan secara acak pada file media dengan algoritma enkripsi, berdasarkan kata sandi yanng dimasukkan. Posisi untuk menyimpan bit pesan akan dipilih secara acak dengan menggunakan teknik acak. Dengan cara ini akan lebih sulit untuk mengetahui keberadaan pesan yang disimpan di dalam (Hamid et al., 2013).

2.3.2 OpenStego

Merupakan *tools* berbasis java, yang memiliki dua fungsi yaitu dapat digunakan untuk menyembunyikan data maupun untuk watermarking. File yang bisa digunakan sebagai media penyimpanan pada tools ini adalah, BMP, GIF, JPEG, JPG, PNG, WNMP. Kemudian file yang telah disisipkan pesan akan disimpan dalam format PNG. OpenStego menyediakan kata sandi untuk meningkatkan keamanan pada file stego (Kunjir et al., 2016).

2.3.3 SilentEye

Tools ini menyediakan antarmuka yang dapat digunakan di semua sistem operasi dengan tampilan yang cukup bagus dan integrasi yang mudah dari algoritma steganografi yang baru. File media yang data digunakan adalah BMP, JPG, PNG, GIF, TIF dan WAV. *Tools* ini juga terdapat fitur penambahan

kata sandi untuk file dengan format BMP dan JPG (Kunjir et al., 2016).

2.3.4 Steg

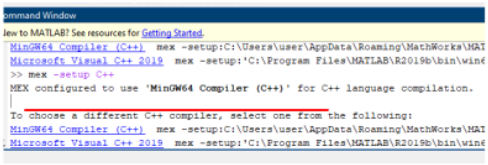
Tools yang ditulis dengan bahasa C++ ini sangat mudah digunakan karena bersifat *portable*. *Tools* Steg ini menggabungkan teknik steganografi dan kiptografi untuk menyembunyikan pesan. Format gambar yang dapat digunakan sebagai media adalah JPG, TIF, PNG dan BMP dan format pesan dalam bentuk TXT. File stego dapat disimpam dalam format PNG dan TIF. Kunci kriptografi yang digunakan simetris dan asimetris (Kunjir et al., 2016).

2.3.5 S-Tools

Tools yang dibuat oleh Andy Brown ini memiliki kesamaan dengan HIP, yaitu format file yang dapat digunakan sebagai media adalah GIF dan BMP saja. S-Tools terbilang mudah digunakan karena *interface*-nya dirancang dengan sederhana. Untuk memuat gambar, pengguna hanya perlu menyeret gambar ke sistem. Setelah gambar diseret, sistem akan memberikan inforamsi tentang jumlah (ukuran) file yang dapat ditampung oleh gambar.
Pada S-Tools terdapat langkah pra-pemrosesan untuk mengurangi jumlah entri wrana dengan menggunakan jarak pengukuran untuk mengidentifikasi warna yang serupa dalam hal intensitas. Setelah langkah ini, setiap warna yang tidak signifikan akan dihubungkan dengan dua warna lain yang salah satunya menjadi tempat penyimpanan pesan (Cheddad et al., 2012).

2.4 Implementasi Metode CNN Yedroudj-net

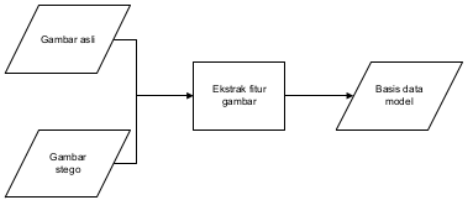
Setelah proses steganografi selesai dengan mengumpulkan semua gambar-gambar stego yang dibutuhkan, maka tahap selanjutnya adalah mengimplementasikan metode CNN Yedroudj-net. Semua gambar yang digunakan adalah gambar warana (RGB), dengan format yang berbeda-beda sesuai dengan keluaran yang dihasilkan dari masing-msing tools steganografi.
Pada penelitian ini metode CNN Yedroudj-net akan diimplementasikan dengan menggunakan MATLAB 2019b dan dengan tambahan compiler yang dapat digunakan di Windows 10, yaitu MinGW-w64. Untuk mengunduh compiler ini dapat mengunjungi situs berikut: www.mathworks.com/matlabcentral/fileexchange/52848-matlab-support-for-mingw-w64-c-c-compiler. MinGW berfungsi untuk menghubungkan atau menjalankan bahasa pemrograman C/ C++. Pada MATLAB MinGW dapat dipanggil dengan menggunakan fungsi mex.
Cara mengaktifkan compiler MinGW pada MATLAB dapat memasukkan kode "mex –setup C++" pada Command Window-nya. Jika kode yang ditulis benar (besar dan kecil huruf diperhatikan), maka konfigurasi MinGW telah berhasil. Pada Command Window MATLAB akan muncul keterangan bahwa mex telah diatur untuk dapat digunakan dengan MinGW64 Compailer (C++), seperti dapat dilihat pada Gambar 3. Jika masih terjadi error atau keterangan tersebut belum muncul, maka kode dari C++ belum bisa dijalankan pada MATLAB. Apabila berhasil dimasukkan dan Fugsi mex berhasil diimplementasikan pada MATLAB, maka kode dari Yedroudj-net sudah bisa dijalankan.



Gambar 3. MinGW64 Compailer (C++)

2.4.1 Melatih Data

Proses melatih data pada dasarnya adalah bertujuan untuk mempelajari atau mengenali bentuk atau model yang ada pada sebuah gambar yang diuji, dalam kasus ini gambar asli dan gambar stego. Agar dapat membedakan keduanya. Pada saat melatih data akan menghasilkan sebuah basis data yang berisi model atau ciri-ciri dari sekumpulan gambar asli dan gambar stego. Basis data inilah yang nanti akan digunakan pada proses selanjutnya, yaitu proses uji coba data. Gambaran dari proses melatih data secara umum dapat dilihat pada Gambar 4.



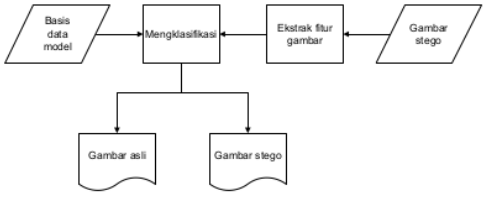
Gambar 4. Gambaran Proses Melatih Data

Skenario pada penelitian ini, tahap awal akan dilakukan proses melatih data (data training). Pada proses melatih data ini bertujuan untuk merancang sebuah prediksi dari sebuah fungsi algoritma yang ada. Dengan kata lain kita melatih sebuah mesin dengan petunjuk yang ada untuk mebuat hasil yang diinginkan. Secara keseluruhan gambar yang digunakan untuk latihan adalah sebanyak 750, terdiri dari 150 gambar dari lima *tools* yang digunakan. Pada bab sebelumnya telah disebutkan proses dari metode CNN Yedroudj-net mulai dari tahap memasukkan data (gambar) awal hingga tahap akhir, yaitu Softmax.

2.4.2 Proses Uji Coba Data

Setelah proses melatih data dilakukan, langkah selanjutnya adalah proses uji coba data, yang bertujuan untuk melihat keakuratan atau kemampuan dari algoritma yang telah dibangun sebelumnya.

Gambar yang akan digunakan adalah 100 untuk masing-masing *tools*. Langkah dari sistem sama dengan langkah yang telah disebutkan sebelumnya. Keluaran dari uji coba data ini nanti akan dibagi ke dalam dua kelas (klasifikasi), yaitu "Gambar Biasa" dan "Gambar Stego". Yang mana, gambar biasa diartikan bahwa pesan rahasia tidak terdeteksi, sedangkan untuk gambar stego adalah pesan rahasia terdeteksi. Gambaran dari proses uji coba dan klasifikasi atau pengelompokan gambar dapat dilihat pada Gambar 5.



Gambar 5. Gambaran Proses Uji Coba Data

Begitu juga untuk uji coba data, dilakukan hal yang sama seperti data latih. Menjalankan kode, dengan memanggil model basis data yang telah dibuat pada proses data latih sebelumnya. Untuk mendapatkan hasil yang jelas, maka akan dilakukan tambahan proses pada tahap ini yaitu pengelompokan kelas atau proses predict image. Di mana terdapat dua kelas, yaitu kelas Gambar Biasa dan Gambar Stego. Potongan hasil dapat dilihat pada Gambar 6.

```
1.bmp adalah "Gambar Stego"
2.bmp adalah "Gambar Stego"
3.bmp adalah "Gambar Stego"
4.bmp adalah "Gambar Stego"
5.bmp adalah "Gambar Stego"
6.bmp adalah "Gambar Stego"
7.bmp adalah "Gambar Biasa"
8.bmp adalah "Gambar Biasa"
9.bmp adalah "Gambar Stego"
10.bmp adalah "Gambar Stego"
11.bmp adalah "Gambar Stego"
12.bmp adalah "Gambar Stego"
13.bmp adalah "Gambar Stego"
14.bmp adalah "Gambar Stego"
15.bmp adalah "Gambar Stego"
16.bmp adalah "Gambar Stego"
17.bmp adalah "Gambar Stego"
18.bmp adalah "Gambar Biasa"
19.bmp adalah "Gambar Stego"
20.bmp adalah "Gambar Stego"
21.bmp adalah "Gambar Stego"
22.bmp adalah "Gambar Stego"
23.bmp adalah "Gambar Stego"
24.bmp adalah "Gambar Stego"
25.bmp adalah "Gambar Stego"
```

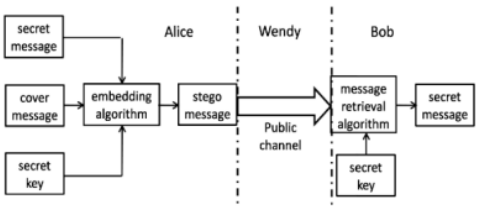
Gambar 6. Tampilan (Sebagian) hasil dari uji coba data

3. LANDASAN TEORI

Secara umum steganalisis terdiri dari dua bagian, yaitu steganalisis aktif dan pasif. Steganalisis pasif hanya menentukan apakah suatu media tertentu adalah stego dengan membandingkan media asli dan stego. Sedangkan aktif akan mencoba mendeteksi panjang pesan dan mengekstraknya, bahkan bisa saja melakukan penghancuran pada pesan dan media stego (Karampidis, Kavallieratou and Papadourakis, 2018) (Samanta, Dutta and Sanyal, 2016).

Berdasarkan tekniknya, steganalisis dibagi menjadi dua, yaitu berdasarkan subjektif (visual) dan statistika (Ge, Huang and Wang, 2011). Teknik subjektif (visual) memanfaatkan indera penglihatan manusia untuk mengamati gambar stego atau yang dicurigai sebagai gambar stego. Contohnya aplikasi StegSpy dan juga algoritma Enhanced LSB. Sedangkan steganalisis dengan teknik statistika merupakan teknik yang menggunakan bantuan matematika untuk melakukan analisa antara citra asli dan citra stego (Ranjan and Forensics, 2016). Metode CNN Yedroudj-net termasuk steganalisis dengan menggunakan teknik statistika.

Steganografi dan steganalisis biasanya digambarkan dengan kasus Prisoner (tahanan penjara) yang dijelaskan oleh Simmons (1984). Gambaran dari kasus ini dapat dilihat pada Gambar 1., yang mana menunjukkan dua orang penghuni penjara (Alice dan Bob) menggunakan teknik steganografi untuk menyembunyikan pesan rahasia yang berisi rencana untuk melarikan diri dari penjara. Selama komunikasi berlangsung keduanya berusaha sebisa mungkin agar rencana mereka tidak diketahui oleh sipir penjara (Wendy). Sedangkan di sisi lainnya, Wendy juga sedang berusaha untuk mendeteksi apakah ada hal yang mencurigakan dari komunikasi yang dilakukan oleh Alice dan Bob (Hidayat, 2011).



Gambar 7. Gambaran umum proses steganilis (Ge, Huang and Wang, 2011)

Berdasarkan tekniknya, steganalisis dibagi menjadi dua, yaitu berdasarkan subjektif (visual) dan statistika(Chen, 2005) (Tsang and Fridrich, 2018). Teknik subjektif (visual) memanfaatkan indera penglihatan manusia untuk mengamati gambar stego atau yang dicurigai sebagai gambar stego. Contohnya aplikasi StegSpy dan juga algoritma Enhanced LSB. Sedangkan steganalisis dengan teknik statistika merupakan teknik yang menggunakan bantuan matematika untuk melakukan analisa antara citra asli dan citra stego. Metode CNN Yedroudj-net termasuk steganalisis dengan menggunakan teknik statistika.

3.1. Blind Steganalysis

Steganalisis blind ini mencoba mendeteksi pesan yang disematkan dengan menggunakan teknik steganografi apapun. Untuk memudahkan penerapan penyerangan ini, digunakan teknik *machine learning* untuk membangun model deteksi dari data eksperimen. Salah satu metode yang telah diterapkan adalah metode *Convolutional Neural Networks* (CNN). Pada steganalisis ini fitur gambar diekstrak dan dikelompokkan dirancang berdasarkan data set pelatihan dari media (gambar) asli dan media stego (Karampidis, Kavallieratou and Papadourakis, 2018)·(Anupama K. Ingale, Nagaraj V.Dharwadkar, 2016)·(Goljan, 2018).

3.2 Metode Yedroudj-Net

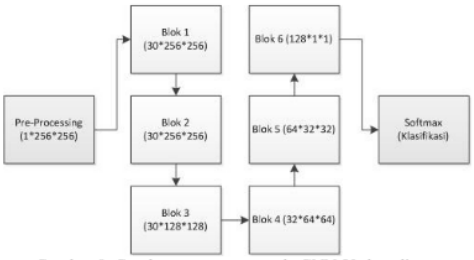
Metode CNN Yedroudj-net ini pada dasarnya sama dengan metode CNN lainnya, tetapi lebih kompleks karena ada beberapa tambahan atau modifikasi pada msing-masing layer. Teknik ini terdiri dari lima blok pra-pemrosesan, lima blok konvolusional, dan blok yang sepenuhnya terhubung yang terdiri dari tiga lapisan yang terhubung sepenuhnya dan terakhir diikuti *softmax*. Jaringan menghasilkan distribusi probabilitas melalui dua label kelas. Blok pra-pemrosesan menyaring gambar asli atau gambar stego dengan *filter high-pass* yang telah ditentukan untuk mengekstraksi residu *noise*.

Gambar yang sudah diproses, kemudian diolah di dalam jaringan. Pra-pemrosesan dengan menggunakan *filter high-pass* sebagian besar dapat menekan konten gambar, memperkecil rentang secara dinamis, dan dengan demikian dapat meningkatkan *signal-to-noise ratio* antara sinyal stego yang lemah dan sinyal gambar asli. Hasilnya, CNN mampu melakukan pembelajaran dari sinyal yang lebih kuat. CNN Yedroudj-net menggunakan 30 filter dasar, untuk memproses gambar input sebelumnya.

Selanjutnya CNN Yedroudj-net dibagi menjadi konvolutional layer yang didedikasikan untuk representasi fitur, yang mengubah gambar input menjadi vektor fitur dan modul klasifikasi yang terdiri dari tiga lapis. Lapisan ini terhubung dengan lapisan *softmax*, yang menghasilkan keputusan klasifikasi apakah gambar merupakan gambar asli atau stego. Sama dengan metode CNN lain seperti Xu-Net (Xu, Wu and Shi, 2016), modul konvolusional memiliki lima blok ditandai dengan Blok 1 sampai Blok 5, untuk mengekstraksi fitur-fitur yang efektif untuk menutupi dan menghentikan diskrimasi gambar. Gambaran umum prosesnya dapat dilihat pada Gambar 8.

Penjelasan Gambar 8:

1. Masukkan gambar (Ukuran: 1 x 256 x 256)
2. Lapisan 0: Konvolusi dengan 30 filter, ukuran 5 × 5, langkah 1, lapisan 2. Ukuran: 30 x 256 x 256
3. Lapisan 1: Konvolusi dengan 30 filter, ukuran 5 × 5, langkah 1, lapisan 2. Ukuran: 30 x 256 x 256 30 kedalaman karena 1 set menunjukkan 1 filter dan ada 30 filter.



Gambar 8. Gambaran umum metode CNN Yedroudj-net

4. Lapisan 2: Konvolusi dengan 30 filter, ukuran 5 × 5, langkah 1, lapisan 2. Ukuran: 30 x 256 x 256
5. Lapisan 3: Penggolongan Rata-rata dengan filter 5 × 5, langkah 2. Ukuran: 30 x 128 x 128
6. Lapisan 4: Konvolusi dengan 64 filter, ukuran 3 × 3, langkah 1, lapisan 1. Ukuran: 32 x 128 x 128
7. Lapisan 5: Pooling Average dengan filter 5 × 5, langkah 2. Ukuran: 64 x 64 x 64
8. Lapisan 6: Konvolusi dengan 128 filter, ukuran 3 × 3, langkah 1, lapisan 1. Ukuran: 64 x 64 x 64
9. Lapisan 7: Pooling Average dengan filter 5 × 5, langkah2. Ukuran: 128 x 32 x 32
10. Lapisan 8: Konvolusi dengan 256 filter, ukuran 3 × 3, langkah 1, lapisan 1. Ukuran: 128 x 32 x 32
11. Lapisan 9: Global-Average-Pooling dengan filter 32 × 32, langkah 1. Ukuran: 128 x 1 x 1 Fungsi aktivasi dan normalisasi batch digunakan di semua blok.

Berbagi informasi untuk meningkatkan kualitas pembelajaran telah dilakukan di banyak kampus di Indonesia. Salah satunya adalah penerapan media pembelajaran online atau disebut juga sebagai E-Learning. E-Learning terus dikembangkan seiring dengan perkembangan teknologi perangkat bergerak. Pembelajaran tidak hanya bisa dilakukan pada komputer desktop saja, namun dapat juga dilakukan menggunakan perangkat bergerak (mobile) (Han and Shin, 2016). Pembelajaran pemrograman juga dapat dilakukan menggunakan sistem E-Learning (Danutama and Liem, 2013; Yulianto and Liem, 2014).

Gamification merupakan suatu proses penggunaan teknik desain dan mekanisme game dalam aplikasi non-game guna mengikat pengguna dalam mencapai tujuan. Pengertian lain dari gamification yaitu sebuah upaya dalam mengimplmentasikan sebuah konsep game yang tepat sehingga dapat memberikan proses yang menyenangkan serta bermanfaat bagi setiap pihak yang terlibat (Romdhoni & Wibowo, 2014). Dalam gamification terdapat beberapa mekanisme game yang akan diterapkan pada aplikasi pembelajaran pemrograman java yaitu point, level user, achievement, dan challenge.

4. HASIL DAN PEMBAHASAN

Setelah dilakukan impelementasi pada metode CNN Yedroudj-net pada MATLAB secara bertahap sesuai dengan yang dijelaskan sebelumnya. Maka selanjutnya adalah mencatat dan menganalisa jumlah gambar yang terdeteksi sebagai stego dan jumlah gambar yang tidak terdeteksi. Hasilnya dapat dilihat dari uji coba yang dilakukan untuk gambar stego dari masing-masing tools steganografi. Dari 100 gambar stego yang diuji coba untuk setiap keluaran tools steganografi, hasil yang diperoleh berbeda-beda. Pada Tabel 2. dapat dilihat hasil dari metode CNN Yedroudj-net untuk masing-masing tools.

Tabel 2. Hasil Pengujian Metode CNNYedroudj-Net

Tools	Hasil	
	Terdeteksi	Tidak Terdeteksi
Hide In Picture	90	10
OpenStego	29	71
SilentEye	88	12
Steg	89	11
S-Tools	85	15

Selanjutnya, uji coba dilakukan dengan tools StegSpy pada 100 gambar stego dari masing-masing tools steganografi. Pada Gambar 9. ditunjukkan hasil terdeteksi dan pada Gambar 10. hasil yang tidak terdeteksi.

Gambar 9. StegSpy (Terdeteksi)

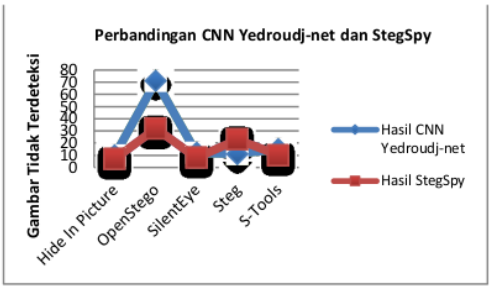
Untuk hasil StegSpy dari masing-masing tools steganografi dapat dilihat pada Tabel 3.

Tabel 3. Hasil pengujian menggunakan tools StegSpy

Tools	Hasil	
	Terdeteksi	Tidak Terdeteksi
Hide In Picture	93	7
OpenStego	68	32
SilentEye	92	8
Steg	87	23
S-Tools	90	10

Gambar 10. StegSpy (Tidak Terdeteksi)

Untuk lebih jelas perbandingan antara CNN Yedroudj-net dan StegSpy dapat dilihat grafik yang ditunjukkan pada Gambar 11.



Gambar 11. Grafik perbandingan CNN Yedroudj-net dan StegSpy

Grafik di atas merupakan nilai atau hasil gambar yang tidak berhasil dideteksi sebagai gambar steganografi dari Yedroudj-net dan StegSpy, yang telah dijabarkan pada Tabel 2. dan Tabel 3. Perbandingan hasil yang diperoleh oleh masing-masing tools dari CNN Yedroudj-net dan StegSpy berbeda-beda.

Dari hasil tersebut, dapat dilihat pada tools OpenStego dan Steg, gambar yang tidak terdeteksi dengan StegSpy lebih tinggi. Sedangkan tiga tools lainnya hasilnya lebih tinggi dengan menggunakan Yedroudj-net. OpenStego dan Steg mengklaim bahwa tools steganografi mereka memiliki tingkat keamanan tinggi dengan ditambahkannya kata sandi pada OpenStego dan Steg menggabungkan teknik steganografi dan kriptografi. Dan kunci kriptografi yang digunakan simetris dan asimetris. Sehingga lebih sulit untuk dideteksi.

Sedangkan untuk metode CNN Yedroudj-net gambar stego yang tidak terdeteksi lebih tinggi dibandingkan dengan tools StegSpy. Hal ini dikarenakan metode CNN Yedroudj-net dirancang untuk mempelajari atau mengenal metode steganagorafi tertentu yang tidak menggunakan tambahan teknik enkripsi (kriptografi). Yang mana tools-tools yang digunakan rata-rata menambahkan fitur enkripsi dalam proses penyisipannya, seperti OpenStego dan Steg. Serta penggunaan kata kunci yang tingkat keamanannya cukup tinggi, yang

terdapat pada kelima tools steganografi yang digunakan pada penelitian ini.

Hasil dengan menggunakan metode CNN Yedroudj-net yang diperoleh lebih rendah. Berdasarkan penjelasan beberapa penelitian sebelumnya ternyata menggunakan basis data yang besar pada metode CNN sangatlah penting, apalagi jika blok yang digunakan berjumlah 5-7 blok seperti pada CNN Yedroudj-net. Meskipun tidak disebutkan jumlah atau angka minimal yang dapat dikategorikan besar itu berapa banyak. Semakin besar basis data yang digunakan, memungkinkan CNN dapat menghasilkan kinerja yang semakin baik pula. Namun, kekurangan dari penggunaan basis data yang besar adalah lamanya waktu yang dibutuhkan untuk melakukan proses pembelajaran.

Dikarenakan kurangnya basis data yang digunakan pada saat melatih data pada penelitian ini, sehingga model yang dihasilkan tidak cukup dinamis dan jelas. Seperti telah dijelaskan pada penelitian sebelumnya bahwa CNN merupakan metode steganalisis yang memanfaatkan fitur-fitur yang dihasilkan dari proses data latih, dan hasil yang diperoleh juga bergantung pada fitur-fitur yang dihasilkan pada basis data model.

Namun dari hasil yang terlihat pada Tabel 3. tools OpenStego menghasilkan gambar yang tidak terdeteksi lebih besar dibandingkan dengan tools steganografi lainnya. Dikarenakan pada tools OpenStego format gambar asli dan gambar stego mengalami perubahan, yaitu dari .jpg menjadi .png. Hal ini dapat mempengaruhi akurasi dari hasil yang diperoleh karena adanya perbedaan fitur-fitur yang akan dihasilkan jika fomat gambarnya berbeda (Yedroudj et al., 2018).

Sedangkan untuk hasil gambar yang tidak terdeteksi sebagai gambar steganografi dengan menggunakan StegSpy lebih sedikit dibandingkan dengan CNN Yedroudj-net, yaitu pada tools HIP, SilentEye dan S-Tools. Untuk OpenStego dan Steg hasil gambar yang tidak terdeteksi lebih banyak. Hal ini dikarenakan OpenStego dan Steg memiliki tingkat keamanan tinggi dengan ditambahkannya kata sandi pada OpenStego dan Steg menggabungkan teknik steganografi dan kriptografi. Dan kunci kriptografi yang digunakan simetris dan asimetris. Sehingga lebih sulit untuk dideteksi(Yedroudj et al., 2018).

StegSpy merupakan tools steganalisis yang dirancang untuk mendeteksi teknik-teknik setgenografi yang umum digunakan, seperti Hiderman, JPHidendSeek, Masker, JPegX dan Invisible Secrets (Choudhary, 2012). Sehingga hasil yang diperoleh untuk pengujian pada lima tools steganografi yang biasa digunakan lebih sedikit gambar yang tidak terdeteksi.

5. KESIMPULAN

Setelah melalui tahap-tahap penelitian pada metode Yedroudj-net terhadap keluaran tools steganografi, maka dapat disimpulkan beberapa hal, yaitu: pada penelitian ini, metode CNN Yedroudj-Net belum bisa dianggap sebagai salah satu metode machine learning dalam steganalisis blind yang baik atau tidak baik. Hal ini dikarenakan basis data yang digunakan pada penelitian ini tidak cukup banyak, sehingga dapat mempengaruhi hasilnya; pada tools StegSpy gambar stego yang tidak terdeteksi lebih sedikit kecuali tools OpenStego dan Steg. Karena kedua tools ini memiliki tingkat keamanan cukup tinggi. Hasilnya lebih tinggi dikarenakan StegSpy memang dirancang untuk mendeteksi teknik steganografi yang umum digunakan, seperti teknik Hiderman, JPHidendSeek, Masker, JPegX dan Invisible Secrets. Untuk kedepannya dapat dilakukan penelitian lebih lanjut dengan menggunakan basis data yang lebih besar lagi dan spesifikasi perangkat komputer yang lebih besar lagi, serta sediakan waktu penelitian lebih lama untuk melakukan proses latih data dengan basis data yang besar.

HAMBATAN PENELITIAN

Beberapa kendala dari penelitian ini adalah jumlah basis data yang tidak banyak, yaitu 150 untuk masing-masing tools. Hal ini dikarenakan waktu yang cukup lama yang dibutuhkan untuk mengumpulkan gambar-gambar dari internet dengan menggunakan Add-Ons DownThemAll pada peramban Firefox. Serta tidak adanya akses untuk mengunduh gambar-gambar dati basis data yang ada di internet. Kendala lainnya adalah perangkat yang digunakan tidak mampu menampung dan melakukan proses melatih gambar dengan jumlah yang besar. Pada penelitian sebelumnya (dengan spesifikasi perangkat yang tinggi dan jumlah data latih sebesar 1000) membutuhkan waktu 1-7 hari lamanya. Sedangkan penelitian ini dengan data latih yang tidak terlalu besar, waktu yang dibutuhkan untuk melakukan proses melatih data 1-3 hari. Dikarenakan spesifikasi perangkat yang digunakan masih cukup rendah dibandingkan dengan penelitian sebelumnya.

Jumlah data latih yang tidak besar mempengaruhi hasil yang diperoleh pada penelitian ini, sehingga hasilnya pengujian dengan menggunakan metode CNN Yedroudj-net lebih rendah dibandingkan dengan tools StegSpy. Meskipun tidak semua tools hasil yang diperoleh lebih rendah.

DAFTAR PUSTAKA

ANUPAMA K. INGALE, NAGARAJ V.DHARWADKAR, P.K., 2016. Universal Steganalysis Using DWT and Entropy Features. *International Conference on Signal and Information Processing (IConSIP)*, pp.1–5.

CHEDDAD, A., CONDELL, J., CURRAN, K. and MCKEVITT, P., 2012. A Comparative Analysis of Steganographic Tools. *School of Computing and Intelligent Systems*, pp.29–37.

CHEN, W., 2005. Study of Steganalysis Methods. *A Thesis Submitted to the Faculty of New Jersey Institute of Technology in Partial Fulfillment of the Requirements for the Degree of Master of*

Science in Electrical Engineering.

CHOUDHARY, K., 2012. Image Steganography and Global Terrorism. *IOSR Journal of Computer Engineering*, 1(2), pp.34–48.

COUCHOT, J.-F., COUTURIER, R., GUYEUX, C. and SALOMON, M., 2016. Steganalysis via a Convolutional Neural Network using Large Convolution Filters for Embedding Process with Same Stego Key. [online] pp.1–24. Available at: <http://arxiv.org/abs/1605.07946>.

GE, H., HUANG, M. AND WANG, Q., 2011. Steganography and steganalysis based on digital image. *Proceedings - 4th International Congress on Image and Signal Processing, CISP 2011*, 1, pp.252–255.

GOLJAN, M., 2018. Blind detection of image rotation and angle estimation. *IS and T International Symposium on Electronic Imaging Science and Technology*, pp.1–10.

HAMID, N., YAHYA, A., AHMAD, R.B., NAJIM, D., KANAAN, L. AND PERLIS, K., 2013. Steganography in image files : A survey. 7(1), pp.35–55.

HIDAYAT, W., 2011. Mendeteksi Keberadaan Pesan Tersembunyi dalam Citra Digital dengan Blind Steganalysis. (Desember), pp.77–81.

KARAMPIDIS, K., KAVALLIERATOU, E. and PAPADOURAKIS, G., 2018. A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, [online] 40, pp.217–235. Available at: <https://doi.org/10.1016/j.jisa.2018.04.005>.

KUNJIR, S.M., PATIL, S.D., JABEEN, S., BHOSALE, S. V and COLLEGE, D.Y.P.A.C.S., 2016. Review On Stenography Tools. *International Research Journal of Engineering and Technology (IRJET)*, 03(10), pp.1223–1225.

PAMUNGKAS, F.G., HIDAYAT, B. and ANDINI, N., 2017. Implementasi Teknik Steganalisis Menggunakan Metode Improvement Difference Image Histogram. pp.1–7.

PIPKORN, D. and WEISBROT, P., 2012. Steganography - The Hidden Message. (Cs 534).

RANJAN, R. AND FORENSICS, C., 2016. Jpeg Image Steganalysis Using Machine. 14(2), pp.96–99.

SAJEDI, H., 2016. Steganalysis based on steganography pattern discovery. *Journal of Information Security and Applications*, [online] 30, pp.3–14. Available at: <http://dx.doi.org/10.1016/j.jisa.2016.04.001>.

SAMANTA, S., DUTTA, S. and SANYAL, G., 2016. A real time text steganalysis by using statistical method. *Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016*, (March), pp.264–268.

TSANG, C.F. and FRIDRICH, J., 2018. Steganalyzing images of arbitrary size with CNNs. *IS and T International Symposium on Electronic Imaging Science and Technology*, pp.1–8.

XU, G., WU, H.Z. and SHI, Y.Q., 2016. Structural design of convolutional neural networks for steganalysis. *IEEE Signal Processing Letters*, 23(5), pp.708–712.

YE, J., NI, J. and YI, Y., 2017. Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Transactions on Information Forensics and Security*, 12(11), pp.2545–2557.

YEDROUDJ, M., COMBY, F., CHAUMONT, M., 2018. Yedrouj-Net : An efficient CNN for spatial steganalysis To cite this version : HAL Id : lirmm-01717550.

Halaman ini sengaja dikosongkan

HASIL CEK_60020397_Point-C39-IRD-85Steganalisis Blind dengan Metode Convolutional Neural Network (CNN) Yedroudj-Net terhadap Tools Steganografi

ORIGINALITY REPORT

4%	5%	0%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	j-ptiik.ub.ac.id Internet Source	1%
2	jtiik.ub.ac.id Internet Source	1%
3	Submitted to Universitas Siliwangi Student Paper	1%
4	doku.pub Internet Source	1%
5	Submitted to Forum Komunikasi Perpustakaan Perguruan Tinggi Kristen Indonesia (FKPPTKI) Student Paper	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		