SCIENCE AND INFORMATION TECHNOLOGY
SINTECH
JOURNAL

SINTECH JOURNAL | ISSN 2598-7305 | E-ISSN 2598-9642
Vol. 6 No 1 – April 2023 | https://s.id/sintechjournal
DOI : https://doi.org/10.31598
Publishing : Prahasta Publisher

Implementasi Steganografi Gambar Menggunakan Algoritma Generative Adversarial Network

Gilang Miftakhul Fahmi[1], Khairunnisak Nur Isnaini*[2], Didit Suhartono[3]
[1,2,3]Departemen Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto
Jl. Letjend Pol. Soemarto No. 126, Purwokerto, Indonesia

e-mail: gilangfahmi20@gmail.com[1], nisak@amikompurwokerto.ac.id*[2], didit@amikompurwokerto.ac.id[3]

Received : March, 2023	Accepted : April, 2023	Published : April, 2023

Abstract

In the era of information technology, it is very important to protect data and information so that it will not be misused by unauthorized parties. One of the techniques to secure data is steganography. Nevertheless, steganography techniques can still be detected by steganalysis techniques. Steganalysis is a technique that is used to analyze hidden messages in steganography. Hence, this study applies image processing techniques with the Generative Adversarial Network algorithm model which aims to manipulate images so that steganalysis techniques cannot detect hidden messages. The application of Generative Adversarial Network algorithm is examined by using a web-based application containing message hiding and extraction functions. It was proven that the Generative Adversarial Network algorithm can be applied to create mock objects. Images can be revived based on training data which is used as a model to know how the algorithm works. In addition, it is showed that the Generative Adversarial Network algorithm were successfully applied to image steganography and can be functioned to prevent steganalysis techniques in detecting messages in images. The difference of metadata in cover image and stego image are seen in their size from 353 to 576 and their bit depth from 8 to 24. Further research is expected to be able to select steganographic images beyond the training data model that accordance to the original size and are chosen randomly according to the selection of the user.

Keywords: *Steganography Steganalysis, Image Processing, Generative Adversarial Network*

Abstrak

Pada era teknologi informasi sangat penting dalam menjaga data dan informasi supaya tidak disalahgunakan pihak yang tidak bertanggung jawab. Salah satu teknik mengamankan data yaitu steganografi. Namun, teknik steganografi masih dapat dideteksi dengan teknik steganalisis. Steganalisis merupakan teknik untuk menganalisis adanya pesan tersembunyi pada steganografi. Oleh karena itu penelitian ini menerapkan teknik image processing dengan model algoritma Generative Adversarial Network yang bertujuan untuk memanipulasi gambar sehingga pesan tersembunyi tidak dapat dideteksi oleh teknik steganalisis. Pembuktian hasil penerapan algoritma Generative Adversarial Network menggunakan aplikasi berbasis web yang berisi fungsi penyembunyian pesan dan ekstraksi pesan. Hasil yang diperoleh yaitu algoritma Generative Adversarial Network dapat diterapkan untuk membuat objek palsu dan citra gambar dapat dibangkitkan kembali berdasarkan pelatihan data yang menjadi model cara kerja algoritma. Selain itu, pada hasil pengujian algoritma Generative Adversarial Network berhasil diterapkan pada steganografi gambar yang berfungsi mencegah teknik steganalisis dalam upaya mendeteksi pesan di dalam gambar. Adanya perbedaan metadata pada cover image dan stego image terlihat pada size yang semula 353 menjadi 576 bytes dan bit depth dari 8 ke 24. Penelitian selanjutnya diharapkan dapat memilih gambar steganografi selain hasil dari model data latih sesuai dengan ukuran asli yang dipilih secara acak sesuai pemilihan dari pengguna.

Kata Kunci: *Steganografi, Steganalisis, Image Processing, Generative Adversarial Network*

1. PENDAHULUAN

Berkembangnya teknologi informasi membuat informasi dan komunikasi semakin cepat dan mempermudah perkerjaan [1]. Namun, perkembangan informasi dan komunikasi tidak selalu memberikan kenyamanan dan keamanan terutama pada data pengguna [2]. Pentingnya keamanan data sebagai bentuk menjaga dan melindungi data yang berbentuk data digital seperti video, foto, audio dan teks agar terhindar dari kejahatan dalam penyalahgunaan data digital [3].

Data digital dapat dilindungi salah satunya menggunakan teknik steganografi [4]. Steganografi adalah sebuah metode yang bertujuan untuk mengamankan dan menyisipkan pesan ke dalam data digital salah satunya gambar, sehingga pesan tidak bisa dibaca oleh sembarang orang kecuali penerima yang dituju [5]. Keamanan data digital tidak sepenuhnya berdampak positif bagi pengguna. Salah satu dampak negatif kasusnya yaitu pada kasus peredaran narkoba kelompok *Al-Qaeda* menggunakan steganografi dengan mengirimkan pesan yang disisipkan kedalam sebuah gambar [6][7]. Pesan yang dapat disisipkan kedalam gambar disebut dengan steganografi gambar [8]. Pada steganografi gambar pesan gambar asli disebut *cover image*, sedangkan gambar yang telah disisipi pesan disebut *stego image* [9].

Steganografi pada gambar bertujuan untuk mengamankan pesan didalam gambar [10]. Namun, steganografi gambar sering kali dapat dideteksi oleh teknik steganalisis yang berfungsi untuk mendeteksi adanya pesan tersembunyi pada *stego image* [11]. Steganalisis adalah sebuah kegiatan untuk menganalisis yang bertujuan untuk mendeteksi adanya teknik steganografi pada data digital salah satunya gambar [12]. Oleh karena itu, diperlukan adanya teknik untuk melapisi keamanan untuk menjaga data tersebut agar tidak terdeteksi.

Salah satu teknik agar terhindar dari steganalisis menggunakan *image processing* [13]. *Image Processing* merupakan proses memanipulasi gambar yang bertujuan untuk menyempurnakan informasi pada gambar [14]. Algoritma yang dapat digunakan untuk memanipulasi gambar salah satunya menggunakan algoritma *deep learning* generatif yaitu *Generative Adversarial Network* (GAN) [15].

Generative Adversarial Network merupakan salah satu algoritma deep learning generatif untuk membuat data baru menyerupai data training sehingga membentuk data yang baru [16]. *Algoritma* GAN bertujuan untuk mengamankan informasi pada gambar [17].

Pada penelitian sebelumnya [18] membahas tentang steganalisis menggunakan algoritma GAN yang berfungsi untuk mengacak atau memanipulasi pesan sehingga pesan yang disembunyikan tidak dapat terdeteksi oleh steganalisis. Cara kerja algoritma GAN berasal dari dua komponen utama yaitu generator dan discriminator [19]. Pada generator berfungsi menghasilkan data palsu sedangkan pada discriminator membedakan data asli dan data palsu yang berasal dari data training [19].

Pada penelitian sebelumnya [20] berhasil memanipulasi gambar yaitu pada gambar medis sinar-x dengan mengecilkan ukuran penyimpanan gambar, namun gambar yang dihasilkan tetap terlihat dengan jelas melalui perbandingan algoritma *Run Length Encoding, Huffman,* dan *Lempel Ziv Welch*. Pada saat memanipulasi gambar tidak hanya dengan mengecilkan ukuran gambar contohnya dengan meningkatkan kontras pada gambar atau mengubah dan menambahkan objek pada gambar [21][22].

Pada penelitian sebelumnya [23] menggunakan metode *Least Significant Bit* sebagai metode penyisipan pesan dengan 8 bit pada aplikasi steganografi gambar berbasis desktop. Penelitian selanjutnya [24] mengungkapkan bahwa teknik penyembunyian pesan pada gambar atau steganografi gambar dapat dideteksi oleh teknik steganalisis, sehingga keamanan pada pesan yang disembunyikan terancam. Selanjutnya penelitian [25] menerapkan algoritma GAN pada steganografi gambar sebagai metode yang bertujuan untuk mengacak atau memanipulasi pesan yang ada pada data digital berupa audio sehingga tidak mudah dideteksi oleh teknik steganalisis.

Penelitian lain yang diungkap oleh [26] membuat aplikasi penyimpanan data menggunakan metode pengembang perangkat

lunak *Extreme Programming* dalam merancang dan membangun aplikasi berbasis web. Keunggulan metode XP adalah dapat melakukan pembaruan tanpa berdampak pada sistem yang telah dibangun [27].

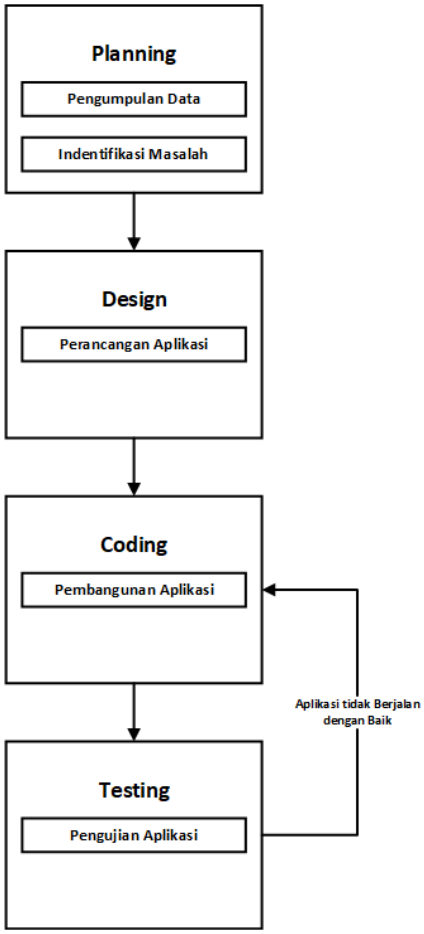
Tujuan penelitian ini adalah untuk mengetahui hasil penerapan model algoritma GAN sehingga pesan yang tersembunyi pada gambar tidak terdeteksi. Penerapan penelitian ini dilakukan ke dalam aplikasi berbasis website. Penelitian ini akan menjabarkan penerapan algoritma GAN yang ada di dalam proses pesan yang dienkripsi hingga pesan yang disembunyikan serta pesan yang dikembalikan dalam bentuk semula sehingga bukan secara khusus membahas algoritma yang diterapkan.

2. METODE PENELITIAN

Dalam penelitian ini penulis akan merancang dan membangun aplikasi steganografi dengan menerapkan algoritma GAN melalui aplikasi berbasis web. Dalam merancang dan membangun aplikasi berbasis web membutuhkan metode perangkat lunak salah satunya menggunakan *Extreme Programming* (XP). Metode XP memiliki tahapan meliputi *planning, design, coding, dan testing*. Pada penelitian ini memiliki alur penelitian yang diadopsi dari metode pengembang perangkat lunak XP.

Penelitian ini dilakukan karena saat ini masih marak terjadi pesan yang telah disembunyikan masih mampu ditembus oleh teknik steganalisis meskipun telah menggunakan beragam teknik kriptografi dan steganografi. Selain itu, pada penelitian sebelumnya belum banyak yang mengungkap teknik penyembunyian pesan yang dikombinasikan dengan sebuah algoritma deep learning khususnya pada fungsi algoritma yang dapat mengamankan sebuah informasi.

Hasil penerapan dapat berupa gambar palsu yang selanjutnya dibangkitkan kembali berdasarkan citra gambar yang telah dilatih. Hasil penerapan algoritma GAN akan dibuktikan menggunakan aplikasi berbasis web.



Gambar 1. Alur Penelitian

Metode penelitian dapat dilihat pada gambar 1 yang merupakan diagram alir penelitian yang diapdopsi dari kerangka kerja *Extreme Programming*. Pada tahap pertama yaitu *planning* terdiri dari pengumpulan data dan identifikasi masalah. Tahap *design* yaitu merancang aplikasi Selanjutnya pada tahap

coding memiliki tahapan pembangunan aplikasi. Tahap akhir yang dilakukan yaitu *testing* yaitu tahapan pengujian aplikasi.

2.1 Pengumpulan Data

Pada penelitian ini menggunakan dua teknik yaitu studi dokumen dan studi pustaka. Studi dokumen yang dilakukan dengan mengumpulkan data gambar secara acak yang digunakan sebagai *cover image* pada aplikasi steganografi. Studi Pustaka dilakukan dengan mengumpulkan berbagai sumber seperti jurnal, buku dan artikel terkait tentang steganografi, steganalisis dan algoritma GAN.

2.2 Identifikasi Masalah

Pada tahap analisis, menganalisis permasalahan, kemudian menentukan solusi yang akan dibuat pada penelitian.

2.3 Perancangan Aplikasi

Pada tahapan ini memvisualisasikan perancangan aplikasi menggunakan metode UML dan perancangan antarmuka. Pemilihan metode UML karena membantu penulis memvisualisasikan perancangan aplikasi secara efektif yang dapat bermanfaat bagi berbagai pemangku kepentingan aplikasi [28].

Pada UML yang dibuat akan menggambarkan setiap proses penerapan algoritma GAN yang digunakan pada proses enkripsi dan deskrips pesan. Proses tersebut dimulai dengan visualisasi alur algoritma GAN yang dijabarkan dengan bentuk arsitekturnya maisng-masing. Selain itu, terdapat visualisasi teknik penyembunyian pesan yang digunakan yaitu LSB yang dapat menggabarkan proses gambar yang masuk dapat berubah ke dalam beberapa layer.

2.4 Pembangunan Aplikasi

Tahap pembangunan aplikasi web dibuat berdasarkan hasil analisis sebelumnya. Pada tahap ini dilakukan coding untuk menerapkan perancangan dan pembangunan aplikasi. Selain itu, pada tahap ini akan dilakukan penerapan algoritma GAN dalam membuat aplikasi steganografi.

Pada tahap ini library python stegano akan dikombinasikan dengan model agoritma GAN. Library python merupakan *library* steganografi pada python yang dapat mempermudah proses pembuatan aplikasi dalam menyembunyikan pesan dengan metode LSB. Selanjutnya *library* tersebut di kombinasikan dengan model algoritma GAN meliputi generator dan discriminator.

2.5 Pengujian Aplikasi

Pada tahap pengujian aplikasi dilakukan dengan cara penyembunyian pesan dan ekstraksi pesan. Pengujian dilakukan dalam dua bentuk yaitu pengujian keberhasilan aplikasi berbasis web dalam merespon uji enkripsi pesan dan deskripsi pesan dari algoritma GAN yang telah diterapkan. Pengujian lain dalam bentuk metadata gambar yang menjadi tempat penyembunyian pesan.

3. HASIL DAN PEMBAHASAN

Penelitian ini berfokus pada pengamanan data berupa teks yang disembunyikan ke dalam gambar atau steganografi gambar dan tidak membahas algoritma *Generative Adversarial Network* dasar secara menyeluruh. Aplikasi steganografi ini berbasis web yang memiliki fungsi utama yaitu mengamankan pesan yang tersembunyi kedalam gambar dan menampilkan Kembali pesan yang telah disisipkan. Berikut hasil dari pembahasan yang telah dilakukan.

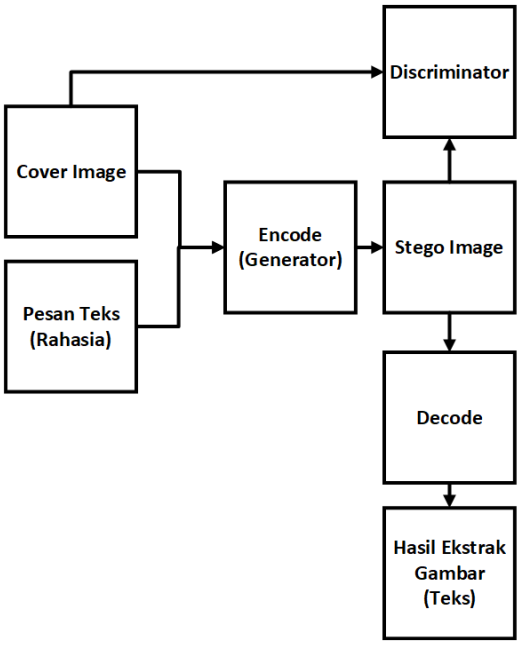
3.1 Pembuatan Aplikasi

a. Planning

Pada penelitian ini membuat aplikasi steganografi gambar berbasis web menggunakan metode *Least Significant Bit* dikombinasikan dengan algoritma *Generative Adversarial Network* yang berfungsi untuk memanipulasi keberadaan pesan berupa teks yang telah tersembunyi pada gambar. Setelah masalah telah didapatkan kemudian menentukan kebutuhan sistem yang meliputi penyembunyian pesan dan ekstraksi pesan.

b. Design

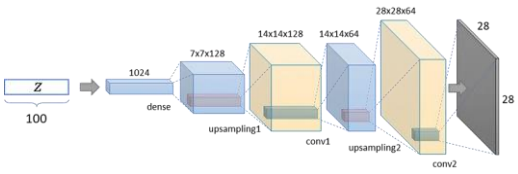
Tahapan *design* merupakan tahap setelah mendapatkan analisis kebutuhan pada tahapan sebelumnya. Perancangan aplikasi terdiri dari perancangan alur sistem. Berikut alur sistem yang dapat dilihat pada gambar 2.



Gambar 2. Alur Sistem Penerapan GAN

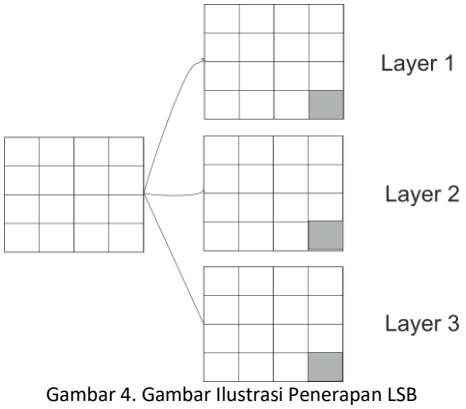
Pada gambar 2 merupakan proses terjadinya penyembunyian pesan dan ekstraksi pesan. Pada penyembunyian pesan proses yang terjadi yaitu memasukan gambar dan teks dan terjadinya penerapan algoritma GAN dasar yang terdiri dari 3 arsitektur encode, discriminator dan decode.

Pada encode merupakan tahap untuk menyembunyikan pesan berupa teks kedalam gambar sekaligus penerapan algoritma GAN yaitu generator. Berikut merupakan arsitektur generator pada penerapan GAN.



Gambar 3. Arsitektur Generator

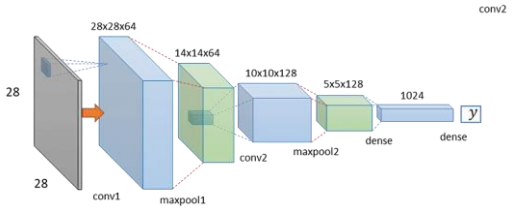
Gambar 3 pada arsitektur generator pada GAN yang menerapkan *Convolutional Neural Network* sebagai generator. Pada proses generator berfungsi menerima input noise sekaligus proses menyisipkan pesan rahasia menggunakan teknik LSB. Gambar 4 merupakan gambar ilustrasi proses LSB yang terjadi ketika gambar dilebur menjadi beberapa layer.



Gambar 4. Gambar Ilustrasi Penerapan LSB

Gambar 4 merupakan ilustrasi penerapan teknik LSB dengan merubah setiap *pixel* yang redundan pada setiap layer untuk menyimpan pesan yang terjadi pada proses generator terutama menggunakan CNN didalamnya.

Sedangkan pada discriminator juga menerima gambar asli dan gambar sintetis dari generator. Pada gambar 5 merupakan ilustrasi arsitektur discriminator.



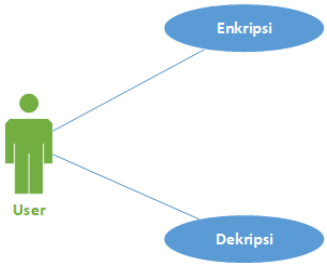
Gambar 5. Arsitektur Diskriminator

Pada gambar 5 arsitektur discriminator menerima inputan dan menghasilkan angka biner kemudian membedakan antara gambar asli dan gambar sintetis yang menunjukkan seberapa besar kemungkinan sebuah gambar adalah asli. Selanjutnya discriminator berfungsi mengambil *cover image* dan *stego image* untuk membedakan dan menyimpan gambar yang telah dimasukan berisi gambar rahasia.

Pemodelan visualisasi sistem dengan menggunakan metode UML (*Unified Modeling Language*) dan membuat *User Interface* sebagai rancangan tampilan aplikasi.

1) *Use Case*

Use case merupakan model yang digunakan untuk menggambarkan interaksi pengguna dengan sistem secara ringkas [29]. Berikut gambar *use case* yang dapat dilihat pada gambar 6.

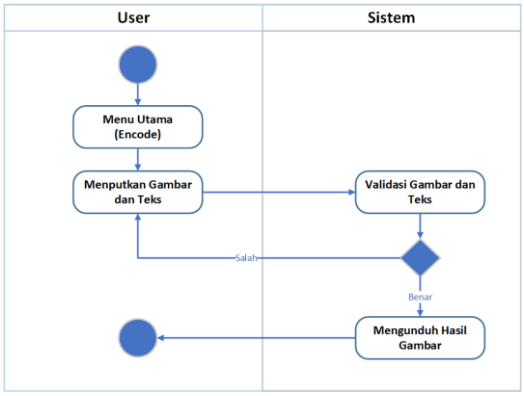


Gambar 6. *Use Case*

Pada gambar 6 *use case* pengguna dapat melakukan dua aksi yaitu penyembunyian pesan dan ekstraksi pesan. Pada penyembunyian pesan *user* dapat memasukan gambar sebagai *cover image* dan menyisipkan pesan kedalam *cover image* berupa teks.

2) Diagram Activity

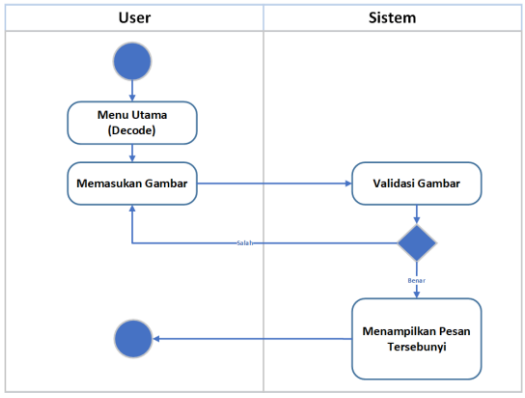
Sedangkan *diagram activity* merupakan diagram yang menggambarkan alur kerja dari tindakan yang dilakukan oleh pengguna. Gambar 7 merupakan gambar *diagram activity* penyembunyian pesan yang dapat dilihat sebagai berikut.



Gambar 7. *Diagram Activity* Penyembunyian Pesan

Pada gambar 7 merupakan gambar *diagram activity* penyembunyian pesan pada sistem yang akan dibuat. Pada tampilan penyembunyian pesan, pengguna memasukan gambar dan teks yang akan disembunyikan. Pada sistem aplikasi yang akan dibuat memilki 3 arsitektur yaitu encoder, decoder dan dekriminator. Pada Enkoder dapat menyembunyikan pesan berupa gambar dengan warna dan bentuk yang sama. Berikut alur penerapan algoritma *Generative Adversarial Network.*

Pada decode merupakan ekstraksi pesan yang telah disembunyikan pada gambar. Berikut merupakan *diagram activity* ekstraksi pesan pada gambar 5.

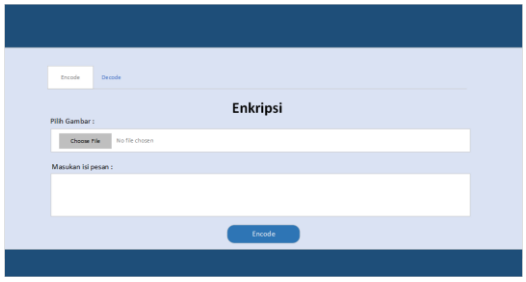


Gambar 5. *Diagram Activity* Ekstraksi pesan

Pada gambar 5 *diagram activity* ekstraksi pesan merupakan alur proses ekstraksi pesan yang tersembunyi pada gambar dengan memasukan gambar pada sistem.

3) User Interface

Pada tahap ini perancangan tampilan sesuai dengan kebutuhan sistem meliputi tampilan penyembunyian pesan dan ekstraksi pesan. Berikut penerapan antarmuka yang digunakan untuk proses menyembunyikan pesan teks kedalam gambar.



Gambar 6. Antarmuka Penyembunyian pesan

Pada gambar 6 antarmuka penyembunyian pesan berfungsi sebagai tampilan memasukan gambar dan pesan yang berupa teks.

c. Coding

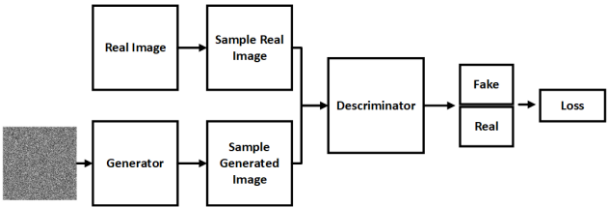
Tahapan *coding* yaitu tahapan untuk menerapkan *design* kedalam bahasa

pemrograman python. *Library* python yang digunakan yaitu stegano, berfungsi sebagai alat menyisipkan pesan dengan menggunakan metode *Least Significant Bit* (LSB). Berikut merupakan penerapan *library* stegano pada coding yang dapat dilihat pada gambar 8.

```
from stegano import lsb
```

Gambar 8. *Library* Steganografi

Gambar 8 merupakan *library* steganografi pada python yang dapat mempermudah proses pembuatan aplikasi dalam menyembunyikan pesan dengan metode LSB. Selanjutnya *library* tersebut di kombisanikan dengan model algoritma GAN meliputi generator dan discriminator. Berikut merupakan arsitektur GAN pada gambar 9.



Gambar 9. Arsitektur GAN

Pada gambar 9 arsitektur GAN, generator membuat gambar palsu dari gambar yang sudah diinputkan sedangkan pada discriminator sebagai pembanding dan membangkitkan citra. Berikut merupakan penerapan implementasi model yang telah dibuat sebelumnya dapat dilihat pada gambar 10.

```
def init():
    global generator
    global discriminator
    global X_train
    generator = load_model('static/models/generator.h5')
    discriminator = load_model('static/models/discriminator.h5')
    (X_train, _) = mnist.load_data()
```

Gambar 10. Penerapan Model GAN

Pada gambar 10 penerapan model GAN merupakan cara untuk memuat model yang sudah dibuat sebelumnya. Dalam menerapkan steganografi dan algoritma GAN terdapat 2 sistem yaitu penyembunyian pesan dan ekstraksi pesan. Pada penyembunyian pesan citra akan diproses pada generator Bersama dengan teks yang akan disembunyikan. Berikut merupakan coding pada proses penyembunyiaan pesan.

```
def encode(container, information):
    img = Image.open(container)
    width, height = img.size
    img_matr = np.asarray(img)
    img_matr.setflags(write=True)
    red_ch = img_matr[:, :, 0].reshape((1, -1))[0]
    information = np.append(information, BaseStego.DELIMITER)
```

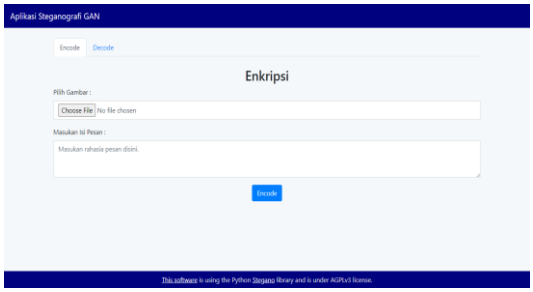
Gambar 11. Coding proses penyembunyian pesan

Pada gambar 11 proses penyembunyian pesan gambar akan disamakan dengan size yang sama dengan data training yang sudah ada sehingga proses penyembunyian pesan dapat berjalan secara normal. Selanjutnya untuk mengetahui isi pesan yang ada membutukan proses ekstraksi pesan. Sedangkan pada gambar 12 merupakan cosing ekstraksi pesan.

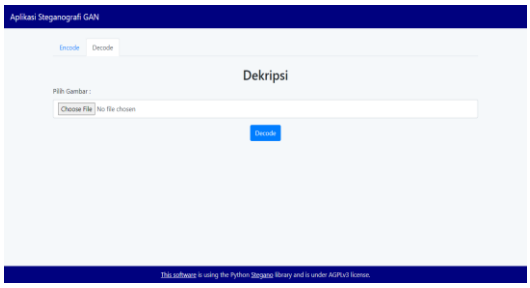
```
def decode(container):
        img = Image.open(container)
        img_matr = np.asarray(img)
        red_ch = img_matr[:, :, 0].reshape((1, -1))[0]
        delim_len = len(BaseStego.DELIMITER)
```

Gambar 12. Coding Ekstraksi Pesan

Pada proses ekstraksi pesan gambar kebalikan dari proses penyembunyian pesan yang akan dibangkitkan kembali dengan data latih yang sudah ada. Berikut merupakan halaman penyembunyian pesan dan ekstraksi pesan yang dapat dilihat pada gambar 13 dan gambar 14.



Gambar 13. Halaman Penyembunyian Pesan



Gambar 14. Halaman Ekstraksi Pesan

Gambar 13 halaman penyembunyian pesan merupakan hasil akhir pembuatan aplikasi

steganografi web yang dapat digunakan pengguna untuk proses penyembunyian pesan dengan memasukan gambar dan teks yang akan disembunyikan. Sedangkan gambar 14 halaman ekstraksi pesan merupakan hasil tampilan yang dapat digunakan oleh pengguna untuk menampilkan pesan yang telah tersembunyi pada gambar.

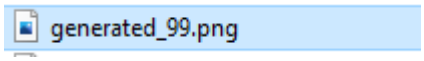
d. Testing

Pada tahapan ini bertujuan untuk menguji aplikasi sehingga aplikasi benar-benar dalam keadaan siap sebelum aplikasi *release*. Pengujian aplikasi meliputi penyembunyian pesan dan ekstraksi pesan.

1) Penyembunyian pesan

Penyembunyian pesan merupakan proses menyisipkan pesan berupa teks kedalam sebuah gambar. Tahapan yang perlu dilakukan dalam alur sistem penyembunyian pesan sebagai berikut.

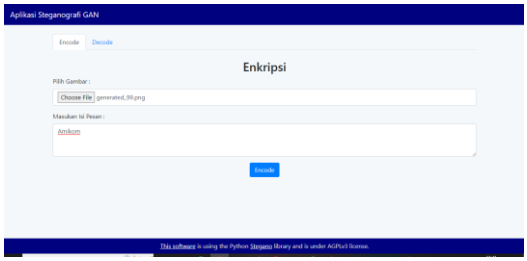
a) Memasukan gambar



Gambar 15. Gambar Inputan

Pada gambar 15 merupakan gambar yang digunakan sebagai tempat untuk menyembunyikan pesan bernama generated_99.png.

b) Masukan pesan yang akan disisipkan yaitu “Amikom” seperti yang terlihat pada gambar 16.



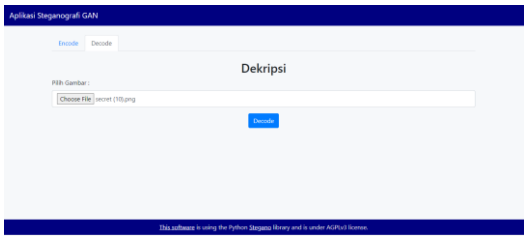
Gambar 16. Proses Penyembunyian pesan

c) Langkah terakhir, klik tombol encode. Maka hasil gambar secara automatis akan terunduh.

2) Ekstraksi pesan

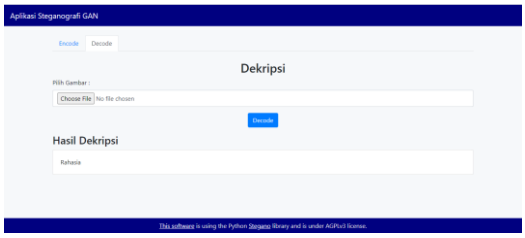
Ekstraksi pesan merupakan proses mengekstraksi pesan yang telah disembunyikan pada gambar sehingga pesan yang telah disembunyikan dapat dibaca oleh penerima pesan. Langkah-langkah dalam proses ekstraksi pesan sebagai berikut.

a) Menginputkan gambar yang telah dipenyembunyian pesan sebelumnya yaitu bernama secret(10).png”



Gambar 17. Memasukan Gambar pada proses ekstrasi pesan

b) Klik decode untuk menampilkan pesan.



Gambar 17. Hasil Ekstraksi pesan

Pada gambar 17 terlihat hasil ekstrasi pesan dan pesan rahasia yang disembunyikan adalah kata Rahasia”.

3.2 Analisis Hasil

Berdasarkan hasil pengujian yang telah dilakukan dapat diperoleh algoritma GAN dapat diterapkan pada aplikasi steganografi berbasis web. Berikut adalah hasil perbandingan gambar asli dan gambar stego yang berasal dari penyembunyian pesan gambar. Gambar asli dan gambar stego yang dapat dilihat pada gambar 18.

Gambar 18. Hasil Gambar Akhir

Pada gambar 18 hasil akhir pada gambar asli dan gambar stego. Perubahan gambar yang

terjadi sedikit karena adanya *loss* (ketidak sesuaian prediksi gambar) pada model algoritma GAN.

Selanjutnya analisis gambar juga dapat dilihat berdasarkan meta data. Hasil meta data sebagai berikut.

Tabel 1. Meta Data

Meta Data	Asli	Hasil
Name	generate_99	secret
Dimentions	28 x 28	28 x 28
Bit Depth	8	24
Size	353 bytes	576 bytes
Format	PNG	PNG

Pada gambar 18 meta data gambar hasil mengalami perubahan setelah disisipi pesan. Perubahan yang terjadi antara lain *bit depth* dan *image size*. *Bit depth* merupakan kedalaman bit yang berfungsi untuk menyimpan informasi pada gambar. *Bit depth* pada gambar asli 8 berubah menjadi 24, selanjutnya pada *size* berubah 353 bytes menjadi 576 *bytes*. Perubahan pada *bit depth* dikarenakan adanya penyembunyian pesan pada gambar yang berupa teks.

4. KESIMPULAN

Berdasarkan hasil dan analisis penerapan algoritma GAN berhasil diterapkan pada steganografi gambar dan membantu meningkatkan teknik penyembunyian pesan, Namun gambar yang dihasilkan belum sempurna terutama pada resolusi gambar. Hal tersebut disebabkan pada saat pemodelan hingga menemukan data set gambar yang tersedia harus memiliki size yang sama sehingga dukungan yang kurang maksimal pada spesifikasi perangkat keras yang digunakan dapat menghambat proses pemodelan data. Hal tersebut menyebabkan proses pemodelan menjadi error.

Penelitian selanjutnya diharapkan dapat meningkatkan kualitas gambar sehingga tidak mengalami banyak perubahan seperti warna, ukuran dan resolusi. Adanya alternatif lain dapat menggunakan google colab dalam pemodelan algoritma GAN dapat memaksimalkan hasil pemodelan data.

DAFTAR PUSTAKA

[1] I. A. Huda, "Perkembangan Teknologi Informasi Dan Komunikasi (Tik) Terhadap Kualitas Pembelajaran Di Sekolah Dasar," *J. Pendidik. dan Konseling*, vol. 2, no. 1, pp. 121–125, 2020, doi: 10.31004/jpdk.v1i2.622.

[2] A. I. Mutiasari, "Perkembangan Industri Perbankan Di Era Digital," *J. Ekon. Bisnis Dan Kewirausahaan*, vol. 9, no. 2, pp. 32–41, 2020, doi: 10.47942/iab.v9i2.541.

[3] N. Nukman, Y. Prayudi, and F. Yudha, "Pengembangan Framework Digital Forensics Investigation (FDFI) Pada Sosial Media Dengan Metode System Development Life Cycle (SDLC)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1852–1860, 2022, doi: 10.35957/jatisi.v9i3.2151.

[4] B. J. Simbolon, "Steganografi Penyisipan Pesan Pada File Citra Dengan Menggunakan Metode LSB (Least Significant Bit)," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 1, pp. 1–6, 2021, doi: 10.32672/jnkti.v4i1.2656.

[5] Y. Aditya, A. Pratama, and A. Nurlifa, "Studi pustaka untuk steganografi dengan beberapa metode," *Semin. Nas. Apl. Teknol. Inf. 2010 (SNATI 2010)*, vol. 2010, no. Snati, pp. 32–35, 2010.

[6] M. B. Akbar and E. V Haryanto, "Aplikasi Steganografi dengan Menggunakan Metode F5," *… Sist. Inf. dan Teknol. …*, no. April 2013, pp. 165–178, 2015, [Online]. Available: https://ejurnal.dipanegara.ac.id/index.php/jusiti/article/view/58.

[7] S. Gallagher, "Steganography: how al-Qaeda hid secret documents in a porn video," *arstechnica.com*, 2012. https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video/ (accessed May 20, 2022).

[8] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb)," *J. Cendikia*, vol. 17, no. 1 April, pp. 194–198, 2019, [Online]. Available: https://jurnal.dcc.ac.id/index.php/JC/article/view/201.

[9] Z. A. I. Niswati, "STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB)ZA'IMATUN, N.; BIT, Steganografi Berbasis Least Significant. Steganografi

Berbasis Least Significant Bit (LSB) Untuk Menyisipkan Gambar Ke Dalam Citra Gambar," vol. 5, no. 2, pp. 181–191, 1979, [Online]. Available: https://journal.lppmunindra.ac.id/index.php/Faktor_Exacta/article/download/194/185.

[10] M. Hadi and N. U. R. Aini, "Gambar Menggunakan Metode Eof Dengan Enkripsi Rsa Berbasis Android," vol. 2, pp. 131–136, 2019.

[11] H. M. Damayanti, Yudo Bismo Utomo, "Penerapan Teknik Steganalysis Menggunakan Metode Chi Square Attack Pada Stego Image Berformat Jpeg Berbasis Android," *J. Sist. Telekomun. Elektron. Sist. Kontrol Power Sist. Komput.*, vol. 1, no. 1, pp. 51–58, 2021, [Online]. Available: https://media.neliti.com/media/publications/344687-implementation-of-steganalysis-technique-2f679bb4.pdf.

[12] W. Hidayat, "Mendeteksi Keberadaan Pesan Tersembunyi dalam Citra Digital dengan Blind Steganalysis," pp. 77–81, 2011.

[13] R. Siringoringo, "Analisis Psnr Pada Steganografi Least Significant Bit Dengan Pesan Terenkripsi Advanced Encription System," *J. Method.*, vol. 2, no. 1, pp. 124–130, 2016.

[14] A. R. Kelrey, Y. Prayudi, and E. Ramadhani, "Identifikasi Source Image Menggunakan Pendekatan Forensic Similarity pada Image Forensik," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1873–1883, 2022, doi: 10.35957/jatisi.v9i3.2483.

[15] A. Zein, "Manipulasi Gambar Menggunakan Jaringan Adversarial Siklus-Konsisten," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 29, no. 2, pp. 1–5, 2019, doi: 10.37277/stch.v29i2.330.

[16] A. A. Praramadhan and G. E. Saputra, "Cycle Generative Adversarial Networks Algorithm With Style Transfer For Image Generation," pp. 1–12, 2021, [Online]. Available: http://arxiv.org/abs/2101.03921.

[17] H. Shi, J. Dong, W. Wang, and Y. Qian, "SSGAN: Secure Steganography Based on Generative Adversarial Networks Haichao," *Pacific Rim Conf. Multimed. Adv. Multimed. Inf. Process.*, vol. PCM 2017, pp. 534–544, 2017, [Online]. Available: http://link.springer.com/10.1007/978-3-642-34778-8--------.

[18] J. Qin, J. Wang, Y. Tan, H. Huang, X. Xiang, and Z. He, "Coverless image steganography based on generative adversarial network," *Mathematics*, vol. 8, no. 9, pp. 1–11, 2020, doi: 10.3390/MATH8091394.

[19] R. W. P. Pamungkas, Rakhmi Khalida, and Siti Setiawati, "Pembuatan Gambar Sintesis Dari Deksripsi Teks Dengan Algoritma Generative Adversarial Network," *Aisyah J. Informatics Electr. Eng.*, vol. 2, no. 2, pp. 111–114, 2020, doi: 10.30604/jti.v2i2.31.

[20] I. B. G. Anandita, I. G. A. Gunadi, and G. Indrawan, "Analisis Kinerja Dan Kualitas Hasil Kompresi Pada Citra Medis Sinar-X Menggunakan Algoritma Huffman, Lempel Ziv Welch Dan Run Length Encoding," *SINTECH (Science Inf. Technol. J.*, vol. 1, no. 1, pp. 7–15, 2018, doi: 10.31598/sintechjournal.v1i1.179.

[21] F. Liantoni and A. Santoso, "Perbaikan Kontras Citra Mammogram Pada Klasifikasi Kanker Payudara Berdasarkan Fitur Gray-Level Co-Occurrence Matrix," *SINTECH (Science Inf. Technol. J.*, vol. 3, no. 1, pp. 46–51, 2020, doi: 10.31598/sintechjournal.v3i1.528.

[22] I. G. R. M. Putra, M. W. A. Kesiman, G. A. Pradnyana, and I. M. D. Maysanjaya, "Identifikasi Citra Ukiran Ornamen Tradisional Bali Dengan Metode Multilayer Perceptron," *SINTECH (Science Inf. Technol. J.*, vol. 4, no. 1, pp. 29–39, 2021, doi: 10.31598/sintechjournal.v4i1.552.

[23] M. Marudin and W. Windarto, "Implementasi Steganografi Least Significant Bit (Lsb) Pada Aplikasi Berbasis Desktop Di Pengembang Properti Bsa Land," *Skanika*, vol. 4, no. 2, pp. 57–62, 2021, doi: 10.36080/skanika.v4i2.2434.

[24] L. Chen, R. Wang, D. Yan, and J. Wang, "Learning to Generate Steganographic Cover for Audio Steganography Using GAN," *IEEE Access*, vol. 9, pp. 88098–88107, 2021, doi: 10.1109/ACCESS.2021.3090445.

[25] Z. Fu, F. Wang, and X. Cheng, "The

secure steganography for hiding images via GAN," *Eurasip J. Image Video Process.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13640-020-00534-2.

[26] A. Anharudin, S. Siswanto, and R. M. Syakira, "Rancang Bangun Data Storage System berbasis Web Dengan Metode Extreme Programming," *J. Tekno Kompak*, vol. 16, no. 1, p. 123, 2022, doi: 10.33365/jtk.v16i1.1454.

[27] E. B. Setiawan and A. Setiyadi, "Model Sistem Rekomendasi Untuk Menciptakan Wirausahawan Baru Menggunakan Metode Saw Dan Teknologi Web," vol. 4, no. 1, pp. 99–105, 2021, [Online]. Available: https://doi.org/10.31598.

[28] H. H. BAHAR, "Perancangan Aplikasi Pemilihan Rumah Kos di Sekitar Universitas Mercubuana dengan metode SAW Berbasis Website," 2022, [Online]. Available: https://repository.mercubuana.ac.id/69145/%0Ahttps://repository.mercubuana.ac.id/69145/1/01 Cover.pdf.

[29] Haviluddin, "Memahami Penggunaan UML (Unified Modelling Language)," *Memahami Pengguna. UML (Unified Model. Lang.*, vol. 6, no. 1, pp. 1–15, 2011, [Online]. Available: https://informatikamulawarman.files.wordpress.com/2011/10/01-jurnal-informatika-mulawarman-feb-2011.pdf.