Jurnal Informatika dan Rekayasa Perangkat Lunak (JATIKA)
Vol. 2, No. 1, Maret 2021, page-page. 16~27

ISSN2723-3367

available online at:http://jim.teknokrat.ac.id/index.php/informatika

UJI KETAHANAN CITRA DIGITAL TERHADAP MANIPULASI ROBUSTNESS PADA STEGANOGRAPHY

Ikwan Pujianto[1], Dedi Darwis[2]
S1 Informatika,Universitas Teknokrat Indonesia[1,2]

Ikwanpuji09@gmail.com[1],darwisdedi@teknokrat.ac.id[2]

Received: (1 Maret 2021)**Accepted**: (18 Maret 2021) **Published:** (30 Maret 2021)

Abstract

In the increasingly sophisticated technological developments, the exchange of information and data on internet media is very easy so that the privacy of such data or information really requires a good security. In the application of security, there are not enough good safeguards, but unique safeguards. Steganography is a technique of hiding messages in a medium for inserting a message or cover image, so that the presence of the secret message that is inserted cannot be seen directly. Algorithm Last significant bit (LSB) is part of a binary data sequence (base two) that has the least significant / smallest value. It is located at the far right of the bit sequence. To test the durability of the algorithm, this test tests the quality of the image after experiencing the steganography process, tests that will be carried out such as imperceptibility and fidelity. Then for testing using the attack will be carried out by attacking the stego image by rotating and resizing the image, then proceed with recovery. From the test results it can be concluded that the percentage of steganographic image resistance to rotate and resize attacks is very weak. Meanwhile, based on the fidelity test results, the quality of the stego image and the original image resulted in an MSE value of 0.03 and a PSNR value of 81.389 dB. Meanwhile, from the imperceptibility test, the image quality is good, because the stego image does not change significantly.

Keywords: Steganography, LSB, resize, rotate, MSE, PSNR

Abstrak

Pada perkembangan teknologi yang semakin canggih, pertukaran informasi dan data pada media internet sangat mudah sehingga privasi sebuah data atau informasi tersebut sangat membutuhkan sebuah pengamanan yang baik. Dalam pengaplikasian pengamanan yang dilakukan tidak cukup pengamanan yang baik, tetapi pengamanan yang unik. Steganografi merupakan teknik menyembunyikan pesan di dalam suatu media penyisipan pesan atau cover image, sehingga keberadaan pesan rahasia yang disisipkan tidak dapat dilihat secara langsung. Algoritma*Last significant bit*(LSB) adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Untuk pengujian ketahanan algoritma, pengujian ini menguji kualitas dari gambar setelah mengalami proses steganografi, pengujian yang akan dilakukan seperti *imperceptibility* dan *fidelity*. Kemudian untuk pengujian menggunakan serangan akan dilakukan dengan menyerang gambar stego dengan rotasi dan resize gambar, kemudian dilanjutkan dengan *recovery*. Dari hasil pengujian dapat ditarik kesimpulan bahwa persentase ketahanan citra steganografi terhadap serangan *rotate* dan *resize* sangat lemah. Sedangkan berdasarkan hasil pengujian *fidelity* kualitas *stego image* dan gambar asli menghasilkan nilai MSE sebesar0,03 dan nilai PSNR mencapai 81,389 *dB*. Sedangkan dari pengujian *imperceptibility* kualitas citra baik, karena *stego image* tidak mengalami perubahan yang signifikan.

Kata Kunci: *Steganografi, LSB, resize, rotate, MSE, PSNR*

To cite this article:
Ikwan Pujianto, Dedi Darwis. (2021). Uji Ketahanan Citra Digital Terhadap Manipulasi *Robustness* pada *Steganography*. *Jurnal Informatika dan Rekayasa Perangkat Lunak*, Vol(2) No(1), 16-27.

PENDAHULUAN

Pada perkembangan teknologi yang semakin canggih, pertukaran informasi dan data pada media internet sangat mudah, sehingga privasi sebuah data atau informasi tersebut sangat membutuhkan sebuah pengamanan yang baik (Ahdan and Setiawansyah 2020; Maulida, Hamidy, and Wahyudi 2020; Rahmanto et al. 2020). Dalam pengaplikasian pengamanan yang dilakukan tidak cukup pengamanan yang baik, tetapi pengamanan yang unik, maksud dari unik disini yaitu pengaman data dengan menggunakan media yang bisa berupa media citra digital, audio ataupun video (Darwis, Pasaribu, and Surahman 2019; Putra 2020). Pengamanan data dengan sebuah media ini tergolong sangat unik memungkinkan penyerang tidak menyadari bahwa pada sebuah media tersebut terdapat sebuah data atau informasi yang di sisipkan. Pengamanan data atau informasi yang menggunakan media citra digital, audio dan video yaitu steganografi (Sulistiani, Triana, and Neneng 2018).

Steganografi merupakan teknik menyembunyikan pesan di dalam suatu media penyisipan pesan atau cover image, sehingga keberadaan pesan rahasia yang disisipkan tidak dapat dilihat secara langsung (Apriani, 2016).

Tujuan utama steganografi adalah untuk menyembunyikan informasi dengan baik, sehingga penerima yang tidak berhak atas informasi tersebut tidak mencurigai media steganografi yang berisi data rahasia yang tersembunyi (Shashikala dan Ajay, 2009). Steganografi citra digital adalah teknik penyematan dan mentransmisikan informasi tersembunyi dalam gambar pembawa (*carriers*) dengan cara rahasia (qi, 2016).

Pada steganografi citra digital dapat digunakan untuk mengirimkan pesan atau informasi rahasia, sehingga steganografi citra harus diuji ketahanan nya terhadap serangan yang mungkin bisa terjadi. Salah satu ukuran kekuatan dalam metode steganografi adalah faktor kekokohan atau ketahanan. Untuk mengetahui kekokohan gambar hasil steganografi, dapat dilakukan pengujian *robustness* untuk menunjukkan kemampuan informasi yang tersembunyi *(payload)* bertahan dari proses *(embedding)* dan ekstraksi, termasuk beberapa manipulasi seperti penyaringan *(filtering)*, pemangkasan *(cropping)*, rotasi *(rotating)*, *dan* kompresi *(compression)*. Kemudian, pengukuran kualitas gambar dilakukan untuk membandingkan antara gambar asli dan gambar yang dimodifikasi. Pengukuran kuantitatif dapat dilakukan menggunakan dua langkah yaitu PSNR *(Peak Signal to Noise Ratio)* dan MSE *(Mean Square Error)* (ujianto, 2015).

Darwis dan Kisworo (2017), melakukan penelitian steganografi untuk menyembunyikan pesan teks menggunakan algoritma *End of File*, dalam tersebut menggunakan algoritma *End of File* dan menyisipkan informasi kedalam media citra digital pada bagian akhir *file* gambar, pada penelitian tersebut dilakukan dua pengujian yaitu, pengujian tanpa serangan dan pengujian dengan menggunakan serangan. Pada pengujian tanpa serangan hanya mengukur dari segi kualitas dan mutu gambar, sesuai dengan skenario pengujian, hasil dari pengujian imperectibility membuktikan bahwa *stego-image* yang dihasilkan dengan metode *end of file* tidak memberikan perubahan signifikan dikarenakan gambar hasil steganografi ini hanya mengubah ukuran gambar bukan merubah piksel maupun intensitas warna sehingga dapat disimpulkan secara kasat mata, indera manusia tidak dapat mendeteksi perubahan gambar tersebut. Dari semua responden yang dimana merupakan mahasiswa yang mengambil bidang ilmu komputer, dilihat dari hasil grafik menunjukan bahwa dari 30 responden menghasilkan 30% menjawab "Iya" dan 70% menjawab "Tidak". Pada proses pengujian tahap fidelity tidak nampak nilai MSE yang hanya menghasilkan nilai "0" dan PSNR menghasilkan nilai "∞" (tak hingga) dikarenakan metode yang digunakan menyisipkan pesan di akhir file tanpa merubah nilai intensitas warna pikselnya sedangkan untuk *recovery* pesan, ekstraksi yang dilakukan dapat mengembalikan pesan secara utuh. Pada Pengujian dengan serangan *robutness* gambar steganografi mengalami penambahan ukuran file jika diputar dengan rata-rata mencapai 74,72 % dan berkurang ukuran file jika mengalami pemotongan dengan rata-rata mencapai 26,73 %, sedangkan untuk proses ekstraksi pesan setelah penyerangan mengalami kegagalan.

Paraskevov et al (2017), melakukan percobaan melakukan penyerangan dengan cara manipulasi putar *(rotate)*, balik *(flip)* atau kombinasi acak, diusulkan oleh mereka dengan penambahan penanda pada *Stego file* untuk mengatasi serangan tersebut. Untuk alasan ini, pemilihan lokasi, ukuran dan jenis penanda merupakan hal yang sangat penting, untuk seleksi dan langkah operasi dari algoritma. Melalui penanda ini bahwa gambar bisa dibawa ke posisi normal. Metode LSB dipilih untuk algoritma *embedding*, tetapi dengan modifikasi kolom yang mewakili perubahan dalam pembacaan matriks piksel gambar. Alasan perubahan dalam arah pembahasan ini adalah untuk menghambat upaya pihak ketiga untuk mengekstraksi/mengenerate pesan. Algoritma ini dapat bekerja dengan kontainer *BMP* dan *PNG* tanpa batasan dalam ukuran, tetapi disarankan bahwa ukuran dari *file carrier* tidak melebihi 500 KB dengan alasan agar file tersebut tidak mencurigakan.

Dalam percobaan ini menggunakan bahasa pemrograman phyton, satu kelebihan dari bahasa itu adalah adanya satu set instrument atau *library* yang mendukung untuk menangani masalah citra *digital*. Basis data yang dibuat dengan volume 100 gambar dalam format *BMP* dan 100 gambar dalam format *PNG* berfungsi sebagai

kontainer. Gambar-gambar ini berukuran hampir sama antara 150-151KB. Pesan teks yang tersembunyi dihasilkan secara acak dengan ukuran 18816 *byte* dan 1837 *byte*, masing-masing ditetapkan sebagai pesan berkapasitas besar *(large msg)* dan pesan berkapasitas kecil *(small msg)*, pesan rahasia disematkan pada gambar yang sama dengan ukuran maksimum untuk file tertentu. Kemudian untuk menghitung probabilitas mendeteksi pesan tersembunyi atau rahasia, dua metode digunakan. Salah satunya adalah c*hi-square* untuk *steganalysis*. Hasil yang diperoleh menunjukkan bahwa metode c*hi-square* mendeteksi pesan tersembunyi di 27% dari *file*, dan yang kedua metode di 34%.

Ujianto, et al, (2015), melakukan penelitian terhadap *cascaded image steganography* dengan meningkatan ketahanan terhadap serangan pada *stegano images*, menggunakan media *citra digital* dengan format *BMP*, dari percobaan yang dilakukan sebelum mengalami penyerangan, nilai PSNR yang dihasilkan sangat bagus, kemudian *file stegano* mendapat beberapa pengujian. Perhitungan nilai PSNR dilakukan untuk mengukur kualitas produk gambar "*Cascaded Image Steganography*". Setelah serangan terjadi, Nilai PSNR yang dihasilkan rendah, itu menunjukkan bahwa citra digital yang dihasilkan kualitas buruk, berbanding terbalik jika PSNR memiliki nilai tinggi, itu berarti mempunyai kualitas gambar yang bagus. Bentuk serangan terhadap *stego image* dalam penelitian ini adalah operasi pengolah gambar, seperti: JPEG Kompresi, Pemfilteran, Rotasi, dan Pemutaran. Perlu penelitian lebih lanjut dalam memperluas metode ini, yang termasuk dalam penelitian gambar dengan stego analisis. Percobaan lain yang perlu dilakukan adalah penggunaan media cover pesan yang berbeda, dan juga penggunaan algoritma steganografi yang lain, apakah itu sama domain atau di domain yang berbeda..

TELAAH PUSTAKA

Citra Digital

Citra adalah suatu suatu gambaran atau kemiripan dari suatu objek. Citra analog tidak dapat direpresentasikan dalam komputer, sehingga tidak bisa diproses oleh komputer secara langsung. Citra digital adalah citra yang yang dapat diolah oleh komputer. Citra yang dihasilkan dari peralatan digital (citra digital) langsung bisa diolah oleh komputer (Andono, 2017).

Steganografi

Steganografi merupakan seni untuk menyembunyikan pesan didalam media digital sedemikian rupa, sehingga orang lain tidak menyadari ada suatu pesan didalam media tersebut (Andono, 2017:77).

Steganografi merupakan teknik menyembunyikan pesan di dalam suatu media penyisipan pesan atau *cover image*, sehingga keberadaan pesan rahasia yang disisipkan tidak dapat dilihat secara langsung (ending dan melisa, 2016).

LSB (*Last Significant Bit*)

Last significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Sedangkan most significant bit adalah sebaliknya, yaitu angka yang paling berarti/paling besar dan letaknya disebelah paling kiri (Andono, 2017).

METODE PENELITIAN

Sampel

Adapun data atau gambar yang akan diuji berupa gambar primer dan gambar sekunder. Gambar primer merupakan gambar yang berasal dari proses pengambilan gambar menggunakan kamera secara langsung. Sementara gambar sekunder adalah gambar-gambar yang diambil atau diunduh dari *internet* (Megawaty et al. 2020).

Teknik Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian ini yaitu sebagai berikut:

1. Tinjauan Pustaka (*Library Research*)
   Dalam penelitian ini penulis melakukan metode kepustakaan yang dilakukan dengan cara membaca buku-buku yang berhubungan dengan *steganography*, keamanan data, dan penyembunyian data. Serta dengan mengutip jurnal-jurnal penelitian yang bersifat *softcopy* (Isnain et al. 2021).
2. Dokumentasi (*Documentation*)
   Merupakan metode pengumpulan data dengan cara membaca, mencatat, mengutip, dan mengumpulkan data-data secara teoritis dari buku-buku dan internet sebagai landasan penyusunan penelitian. Peneliti meminjam buku di perpustakaan, mencari data dari internet juga dilakukan referensi laporan ini (Ariyanti, Satria, and Alita 2020).

Metode Analisis

Kerangka pengujian digunakan untuk membuat alur atau skenario pengujian terhadap implementasi metode yang diterapkan pada pemrograman yang digunakan (Laudhana, Puspaningrum, and Indonesia 2020; Suaidah and Sidni 2018; Wantoro 2021; Wantoro and Priandika 2017). Pada kerangka pengujian ini juga dijelaskan bagaimana proses pengujian dari awal sampai dengan mendapatkan hasil penelitian yang diharapkan.

1. *Imperceptibility*
   Setelah data disisipkan pada suatu media, media yang menjadi *cover* tersebut seharusnya secara kasat mata terlihat sama dengan media yang sebelumnya belum disisipkan data (Pal and Pramanik 2013).
2. *Fidelity*
   Fidelity mengacu pada kemampuan untuk menguji gambar secara akurat, tanpa adanya distorsi visual atau hilangnya informasi (Silverstein and Farrell 1996).
3. *Robostness*
   Steganografi seharusnya tahan terhadap serangan berbentuk *steganalysis* dan/atau manipulasi gambar (Mishra and Mishra 2012).Pengujian *robustness* akan dilakukan dengan cara menyerang *stego image* dengan serangan-serangan *image processing* seperti *image resize* dan *image rotation*.

HASIL DAN PEMBAHASAN

Proses steganografi

Pada penelitian steganografi ini menggunakan bahasa pemrograman *python* dan menggunakan gambar *cover* berformat jpg. Pada proses steganografi terdapat dua tahap yaitu penanaman pesan dan ekstraksi pesan atau pengambilan pesan dari file gambar steganografi.

a. Proses penanaman pesan

Pada proses penanaman pesan akan dilakukan sesuai dengan flowchart penanaman pesan yang sudah dibahas, untuk penulisan perintah pengkodean program dalam bahasa python dapat dilihat pada gambar 2:

```
def genData(data):
    newd = []
    for i in data:
        newd.append(format(ord(i), '08b'))
    return newd

def modPix(pix, data):
    datalist = genData(data)
    lendata = len(datalist)
    imdata = iter(pix)
    for i in range(lendata):
        pix = [value for value in imdata.__next__()[:3] +
               imdata.__next__()[:3] +
               imdata.__next__()[:3]]
        for j in range(0, 8):
            if (datalist[i][j] == '0') and (pix[j] % 2 != 0):
                if (pix[j] % 2 != 0):
                    pix[j] -= 1
            elif (datalist[i][j] == '1') and (pix[j] % 2 == 0):
                pix[j] -= 1
        if (i == lendata - 1):
            if (pix[-1] % 2 == 0):
                pix[-1] -= 1
        else:
            if (pix[-1] % 2 != 0):
                pix[-1] -= 1
        pix = tuple(pix)
        yield pix[0:3]
        yield pix[3:6]
        yield pix[6:9]

def encode_enc(newimg, data):
    w = newimg.size[0]
    h = newimg.size[1]
    u = int(w / 4)
    v = int(h / 4)
    (x, y) = (v, u)
    for pixel in modPix(newimg.getdata(), data):
        print(pixel)
        newimg.putpixel((x, y), pixel)
        if (x == w - 1):
            x = 0
            y += 1
        else:
            x += 1
def encode():
    img = input("Enter image name(with extension): ")
    image = Image.open(img, 'r')
    data = input("Enter data to be encoded : ")
    if (len(data) == 0):
        raise ValueError('Data is empty')
    newimg = image.copy()
    encode_enc(newimg, data)
    h = int(image.size[0] / 4)
    w = int(image.size[1] / 4)
    new_img_name = input("Enter the name of new image(with extension): ")
    newimg.save('encode/'+new_img_name, str(new_img_name.split(".")[1]))
    print('Kunci ekstraksi : ', h,'*',w)
```

Gambar 2 Pengkodean Proses Penanaman Pesan

b. Proses ekstraksi pesan

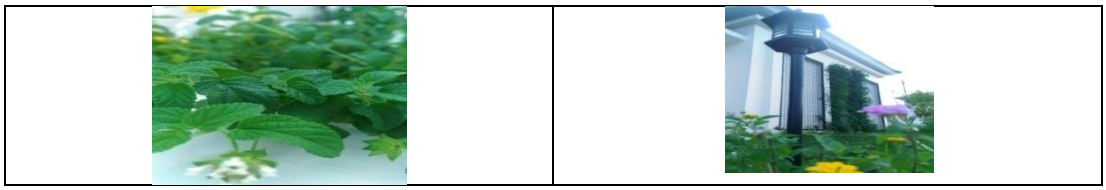
Pada proses setelah penanaman pesan adalah proses ekstraksi pesan, pada proses ini akan dilakuakan pengambilan pesan pada steganografi *images*, untuk penulisan perintah pengkodean program dalam bahasa python dapat dilihat pada gambar 3:

```
gambar = input("Decode Gambar : ")
key = input("Input Key: ")
generate = key.split('*')
a = Image.open(gambar)
x = 1
k = 0
msg = int(generate[2])
for z in range(1, 360):
    img = a.rotate(z)
    width, height = img.size
    u = int(generate[0])
    v = int(generate[1])
    print(u, v)
    new_array = list(img.getdata())
    my_iter = iter(new_array)
    binstr = ''
    data = ''
    x = ''
    y = ''
    c = ''
    m = ''
    for w in range(u, height):
        if w != v:
            u = 0
        m = ''
        for h in range(v, width):
            r = img.getpixel((h, w))
            data = r
            for i in data[:3]:
                if (i % 2 == 0):
                    binstr += '0'
                else:
                    binstr += '1'
            x = binstr
            m = (m,)+r
            c = len(x)
            if c == 9:
                if (m[-1] % 2 != 1):
                    s = chr(int(binstr, 2))
                    y += chr(int(binstr[:-1], 2))
                    binstr = ''
                    k = k+1
                else:
                    k = k + 1
                    if (m[-1] % 2 != 0 & k == msg):
                      y += chr(int(binstr[:-1], 2))
                      print(y)
                      print(m[-1] % 2)
                      exit()
                    else:
                      m = ''
```

Gambar 3 Pengkodean Proses Ekstraksi Pesan

c. Uji ketahanan citra digital steganografi

Uji ketahanan citra digital steganografi bertujuan untuk mengetahui kekuatan dari *file stego* yang didalam nya terdapat pesan rahasia yang tersembunyi, pengujian tersebut dimungkinkan akan memberikan nilai maksimal dari pengujian yang dilakukan. Gambar yang digunakan dalam pengujian ini dapat dilihat pada gambar 4 dan 5



Gambar 4 gambar primer

Gambar 5 gambar sekunder

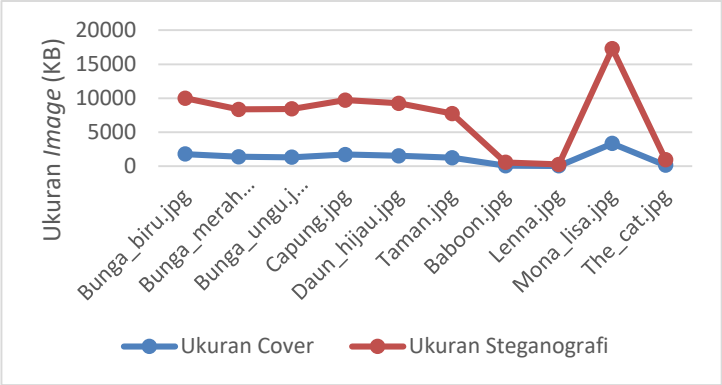
Adapun data atau gambar yang akan diuji berupa gambar primer dan gambar sekunder, seperti yang terlihat pada gambar 4 primer dan gambar 5 Gambar sekunder, gambar primer merupakan gambar yang berasal dari proses pengambilan gambar menggunakan kamera secara langsung. Sementara gambar sekunder adalah gambar-gambar yang diambil atau diunduh dari *internet*.

d. Skenario dan Tahapan Pengujian

Pada pengujian yang dilakukan, akan dibagi menjadi dua pengujian yaitu pengujian tanpa serangan, pengujian ini menguji kualitas dari gambar setelah mengalami proses steganografi, pengujian yang akan dilakukan seperti *imperceptibility* dan *fidelity*. Kemudian untuk pengujian menggunakan serangan akan dilakukan dengan menyerang gambar stego dengan *rotasi* dan *resize* gambar, kemudian dilanjutkan dengan *recovery*.

Tabel 1 Tabel Pengujian Steganografi

No	Nama Gambar *Cover*	Dimensi Gambar *Cover*	Ukuran Gambar *Cover*	Ukuran Pesan	Ukuran Stego
1	Bunga_biru.jpg	2304×4096	1,78 MB	25KB	10MB
2	Bunga_merah.jpg	2304×4096	1,38 MB	25KB	8,36MB
3	Bunga_ungu.jpg	2304×4096	1,31 MB	25KB	8,43MB
4	Capung.jpg	2304×4096	1,71 MB	200KB	9,72MB
5	Daun_hijau.jpg	2304×4096	1,52 MB	200KB	9,25MB
6	Taman.jpg	2304×4096	1,23 MB	25KB	7,73MB
7	Baboon.jpg	512×512	55,6 KB	2,14KB	547KB
8	Lenna.jpg	400×400	25,1 KB	2,14KB	246KB
9	Mona_lisa.jpg	2835×4289	3,34 MB	200KB	17,3MB
10	The_cat.jpg	800×600	135 KB	2,14KB	963KB



Gambar 6 Grafik Hasil Uji Penyisipan Pesan

Tabel 1 dan grafik pada gambar 6 menunjukkan bahwa ukuran file *stego image* lebih besar dibandingkan ukuran gambar *cover* atau gambar sebelum disisipi pesan. Dari gambar 4.1 dapat diperhatikan bahwa bila pesan yang sama disisipkan ke dalam *cover* yang berbeda tetap akan mengalami kenaikan ukuran. Hal ini terjadi dikarenakan saat penyisipan pesan tidak melalui proses kompresi data pesan terlebihi dahulu sehingga mempengaruhi nilai ukuran hasil steganografi.

e. Pengujian tanpa serangan

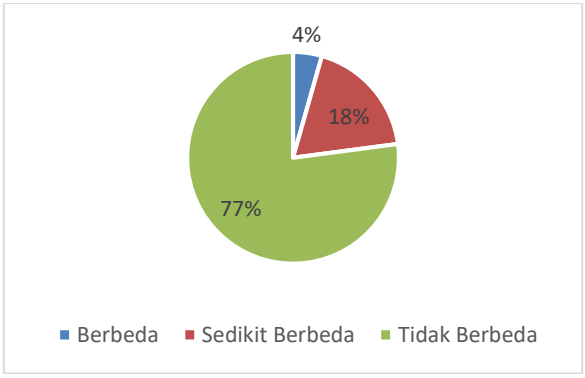
Pengujian tanpa serangan dilakukan untuk mengukur kualitas citra hasil steganografi, sebuah teknik steganografi yang baik setidaknya harus memenuhi kriteria yaitu pesan tahan terhadap serangan berbasis *image processing* (*Robustness*), tidak dapat di bedakan oleh indra pengelihatan manusia (*Imperectibility*), mutu citra hasil steganografi atau *stego image* masih cukup baik (*Fidelity*), dan pesan yang disisipkan dapat diekstraksi kembali (*Recovery*).

1. Imperceptibility

Pengujian *imperceptibility* bertujuan untuk mengetahui seberapa sulit atau mudah *stego image* dapat terdeteksi oleh penglihatan manusia. Pengujian ini dilakukan secara manual dengan melibatkan 45 responden yang diminta untuk mengisi kuisioner dengan membandingkan dan memperlihatkan gambar asli atau gambar *cover* serta gambar yang sudah disisipkan pesan atau *stego image*. Pada kuisioner berisi sejumlah sampel citra seperti pada tabel 2.

Tabel 2 Pengujian *Imperceptibility*

No	Nama Gambar *Cover*	Sangat Berbeda	Berbeda	Sedikit Berbeda	Tidak Berbeda
1	Bunga_biru.jpg	-	3	5	37
2	Bunga_merah.jpg	-	3	6	36
3	Bunga_ungu.jpg	-	2	11	37
4	Capung.jpg	-	2	11	32
5	Daun_hijau.jpg	-	1	4	40
6	Taman.jpg	1	3	8	33
7	Baboon.jpg	-	-	10	35
8	Lenna.jpg	-	2	9	34
9	Mona_lisa.jpg	-	2	10	33
10	The_cat.jpg	-	2	10	33



Gambar 7 Grafik Hasil Pengujian *Imperceptibility*

Pengujian *imperceptibility* mengambil 10 sampel perbandingan gambar *cover* dengan *stego image* dari hasil yang ditunjukkan table 2 responden yang dapat membedakan hasil *stego image* lebih sedikit dibandingkan dengan responden yang tidak dapat membedakan. Dari hasil pengujian ini dapat disimpulkan terdapat perbedaan yang tidak signifikan terhadap hasil steganografi atau antara gambar cover dan gambar steganografi tidak berbeda.

2. Fidelity

Pengujian *fidelity* dilakukan untuk melihat kualitas citra penampung apakah citra mengalami perubahan setelah disisipkan pesan. Pada pengujian ini akan dilakukan beberapa pengujian diantaranya.

1. Pengujian dengan menggunakan 10 gambar *cover*.
2. Pengujian kedua adalah dengan menghitung nilai PSNR dan MSE untuk melihat kualitas citra penampung sebelum dan sesudah disisipkan.

Tabel 3 menunjukkan pengujian terhadap 10 gambar *cover* yang berbeda dengan pesan yang bervariasi.

Tabel 3 Pengujian *Fidelity*

No	Nama Gambar *Cover*	Ukuran Gambar *Cover*	Ukuran Pesan	Ukuran Stego	MSE	PSNR
1	Bunga_biru.jpg	1,78 MB	25KB	10MB	0.0006	89.777
2	Bunga_merah.jpg	1,38 MB	25KB	8,36MB	0.0006	89.813
3	Bunga_ungu.jpg	1,31 MB	25KB	8,43MB	0.0290	73.502
4	Capung.jpg	1,71 MB	200KB	9,72MB	0.0006	89.808
5	Daun_hijau.jpg	1,52 MB	200KB	9,25MB	0.0322	73.058
6	Taman.jpg	1,23 MB	25KB	7,73MB	0.0006	90.185
7	Baboon.jpg	55,6 KB	2,14KB	547KB	0.0124	77.187
8	Lenna.jpg	25,1 KB	2,14KB	246KB	0.0203	75.047
9	Mona_lisa.jpg	3,34 MB	200KB	17,3MB	0.0251	74.128
10	The_cat.jpg	135 KB	2,14KB	963KB	0.0134	76.857

Tabel 3 menunjukan nilai PSNR antara gambar *cover* dan *stego image* sangat baik. Nilai PSNR rata-rata bernilai $80,0\ dB$ yang mana sudah melebihi $40\ dB$, karena semakin besar nilai PSNR semakin baik kualitas citra. Sedangkan nilai *Mean Square Error* (MSE) masih berada di antara 0,5. Ini berarti perubahan kualitas citra asli atau *cover* tidak mengalami perubahan yang signifikan (ujianto, et al, 2015).

f. Pengujian dengan serangan

Pengujian *robustness* dilakukan untuk melihat apakah *stego image* yang telah disisipkan pesan dapat bertahan dari serangan-serangan *image processing*, serta apakah pesan dapat diekstraksi dari *stego image*. Dalam penelitian ini serangan *image processing* yang digunakan adalah *rotasi* dan *resize*.

Tabel 4 Pengujian dengan serangan rotasi

No	Rotasi	Ekstraksi
1	CW 90^0	Gagal
2	CW 180^0	Gagal
3	CW 270^0	Gagal
4	CCW 90^0	Gagal
5	CCW 180^0	Gagal
6	CCW 270^0	Gagal

Kemudian dilanjutkan dengan pengujian dengan *resizestego image*, gambar akan diresize dengan presentase, 10%, 30%, 50% dan 100% dari ukuran gambar stego tersebut.

Tabel 5 Pengujian dengan serangan resize

No	Resize	Ekstraksi
1	10%	Gagal
2	30%	Gagal
3	50%	Gagal
4	100%	Gagal

g. **Pengujian *Recovery***

Pengujian *recovery* dilakukan untuk menguji apakah pesan rahasia yang disisipi pesan pada sebuah gambar dapat kembali dipisahkan dan kembali utuh seperti semula. Pengujian ini dilakukan dengan melihat keutuhan pesan yang diekstraksi dari sejumlah citra uji. Pengujian *recovery* dapat dilihat pada tabel 4.6.

Tabel 6 Pengujian Ekstraksi

No	*Stego Image*	Normal	Rotasi			Resize			
			90^0	180^0	270^0	10%	30%	50%	100%
1	Bunga_biru.jpg	✓	×	×	×	×	×	×	×
2	Bunga_merah.jpg	✓	×	×	×	×	×	×	×
3	Bunga_ungu.jpg	✓	×	×	×	×	×	×	×
4	Capung.jpg	✓	×	×	×	×	×	×	×
5	Daun_hijau.jpg	✓	×	×	×	×	×	×	×
6	Taman.jpg	✓	×	×	×	×	×	×	×
7	Baboon.jpg	✓	×	×	×	×	×	×	×
8	Lenna.jpg	✓	×	×	×	×	×	×	×
9	Mona_lisa.jpg	✓	×	×	×	×	×	×	×
10	The_cat.jpg	✓	×	×	×	×	×	×	×

Note :

- ✓ Recovery Berhasil

- Recovery Gagal

Dapat dilihat dari tabel 4.6 pengujian *recovery* dilakukan dengan cara mengekstrak gambar secara normal, merotasi gambar kemudian diekstrak dan meresize gambar kemudian diekstrak. Dari hasil pengujian *stego image* yang tidak dapat diekstrak adalah *image stego* yang diubah ukurannya (*resize*) dan beberapa rotasi gambar pada gambar. Sedangkan bila *stego image* diekstrak secara normal (tanpa serangan *image processing*) pesan yang tertanam dapat diekstrak dari *stego image*.

h. Konklusi

Pada pengujian yang telah dilakukan didapatkan hasil pengujian yang baik pada kualitas citra digital yang dihasilkan, tetapi pada pengujian serangan masih didapatkan hasil yang kurang memuaskan. Pada pengujian kualitas citra diatas menunjukkan kualitas baik pada gambar dengan format .png tetapi seiring dengan kualitas citra yang dihasilkan juga memperbesar ukuran gambar, hal itu disebabkan karena gambar cover atau gambar asli yaitu berformat .jpg yang memiliki 3 *channel* warna yaitu RGB, sedangkan untuk .png memiliki 3 channel RGB dan ditambah dengan nilai *alpha* atau *alpha channel*. Dibawah ini adalah tabel perbandingan hasil pengujian kualitas citra pada format .jpg dan .png.

Tabel 7 pengujian kualitas gambar stego berformat png.

No	Nama Gambar *Cover*	Ukuran Gambar *Cover*	Ukuran Pesan	Ukuran Stego	MSE	PSNR
1	Bunga_biru.jpg	1,78 MB	25KB	10MB	0.0006	89.777
2	Bunga_merah.jpg	1,38 MB	25KB	8,36MB	0.0006	89.813
3	Bunga_ungu.jpg	1,31 MB	25KB	8,43MB	0.0290	73.502
4	Capung.jpg	1,71 MB	200KB	9,72MB	0.0006	89.808
5	Daun_hijau.jpg	1,52 MB	200KB	9,25MB	0.0322	73.058
6	Taman.jpg	1,23 MB	25KB	7,73MB	0.0006	90.185
7	Baboon.jpg	55,6 KB	2,14KB	547KB	0.0124	77.187
8	Lenna.jpg	25,1 KB	2,14KB	246KB	0.0203	75.047
9	Mona_lisa.jpg	3,34 MB	200KB	17,3MB	0.0251	74.128
10	The_cat.jpg	135 KB	2,14KB	963KB	0.0134	76.857

Tabel 8 pengujian kualitas gambar stego berformat jpg.

No	Nama Gambar *Cover*	Ukuran Gambar *Cover*	Ukuran Pesan	Ukuran Stego	MSE	PSNR
1	Bunga_biru.jpg	1,78 MB	25KB	907 KB	0.0006	89.777
2	Bunga_merah.jpg	1,38 MB	25KB	8,36MB	0.0006	89.813
3	Bunga_ungu.jpg	1,31 MB	25KB	612 KB	0.0290	73.502
4	Capung.jpg	1,71 MB	200KB	9,72MB	0.0006	89.808
5	Daun_hijau.jpg	1,52 MB	200KB	9,25MB	0.0322	73.058
6	Taman.jpg	1,23 MB	25KB	7,73MB	0.0006	90.185
7	Baboon.jpg	55,6 KB	2,14KB	66.1 KB	0.0124	77.187
8	Lenna.jpg	25,1 KB	2,14KB	246KB	0.0203	75.047
9	Mona_lisa.jpg	3,34 MB	200KB	17,3MB	0.0251	74.128
10	The_cat.jpg	135 KB	2,14KB	963KB	0.0134	76.857

Dari perbandingan tabel diatas maka dapat disimpulkan bahwa lebih besar ukuran dan format dari stego tersebut menentukan kualitas citra yang dihasilkan.

SIMPULAN

Modifikasi algoritma LSB yang penulis kembangkan belum dapat menahan serangan *rotate* dan *resize* pada *stego image*, sehingga pesan gagal diekstrak secara utuh. Dari hasil pengujian dapat ditarik kesimpulan

bahwa persentase ketahanan citra steganografi terhadap serangan *rotate* dan *resize* sangat lemah. Namun, bila diekstraksi tanpa menggunakan serangan pesan dapat di ekstraksi dengan baik. Berdasarkan hasil pengujian *fidelity* kualitas *stego image* dan gambar asli menghasilkan nilai MSE sebesar0,03 dan nilai PSNR mencapai 81,389 *dB*. Sedangkan dari pengujian *imperceptibility* kualitas citra baik, karena *stego image* tidak mengalami perubahan yang signifikan.

Dalam algoritma yang penulis kembangkan, pesan yang disisipkan adalah file.txt dengan serangan *rotate* dan *resize*, pada serangan tersebut terdapat pixel yang hilang, sehingga pesan gagal di ekstraksi, saran untuk pengembangan selanjutnya adalah dengan lebih berfokus pada penanganan *recovery pixel* daeri serangan robustness seperti rotasi dan resize atau serangan lainnya. Dari pernelitian yang dilakuakan masih menemui kendala dari segi ukuran file stego yang terlalu besar setelah di sisikan pesan, sehingga ukuran dapat mencapai ukuran yang sangat besar. Untuk pengembangan selanjutnya agar menggunakan kompresi pesan agar file stego hasil steganografi tidak berukuran sangat besar.

.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Penelitian dengan judul "Uji Ketahanan Citra Digital Terhadap Manipulasi *Robustness* pada *Steganography*". Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, sangatlah sulit bagi penulis untuk menyelesaikan Penelitian ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Dr. H.M. Nasrullah Yusuf, S.E., M.B.A., selaku Rektor Universitas Teknokrat Indonesia.
2. Bapak Dr. H. Mahathir Muhammad, S.E., M.M. selaku Dekan Fakultas Teknik dan Ilmu Komputer Universitas Teknokrat Indonesia.
3. Ibu Dyah Ayu Megawaty, S.Kom.,M.Kom. selaku Ketua Program StudiS1 Informatika Fakultas Teknik dan Ilmu Komputer Universitas Teknokrat Indonesia.
4. Bapak Dedi Darwis, S.Kom., M.Kom.selaku Dosen Pembimbing yang telah meluangkan waktu untuk membimbing penulis menyelesaikan skripsi ini.
5. Bapak Zaenal Abidin, S.Si., S.Kom., M.T. selaku Dosen Penguji yang telah meluangkan waktunya untuk menguji seminar skripsi ini.

REFERENSI/DAFTAR PUSTAKA

Ahdan, Syaiful, and Setiawansyah Setiawansyah. (2020). "Pengembangan Sistem Informasi Geografis Untuk Pendonor Darah Tetap Di Bandar Lampung Dengan Algoritma Dijkstra Berbasis Android." *Jurnal Sains Dan Informatika: Research of Science and Informatic* 6(2):67–77.

Ariyanti, Lisa, Muhammad Najib Dwi Satria, and Debby Alita. (2020). "SISTEM INFORMASI AKADEMIK DAN ADMINISTRASI DENGAN METODE EXTREME PROGRAMMING PADA LEMBAGA KURSUS DAN PELATIHAN." *Jurnal Teknologi Dan Sistem Informasi* 1(1):90–96.

Andono, N, P., Sutojo., T., Muljono., 2017, Pengolahan Citra Digital, Andi, Yogyakarta.

Bhattacharyya., S., (2012), "*A Robust Image Steganography using DWT Difference Modulation (DWTDM)*", University Institute of Technology, The University of Burdwan, West Bengal, India.

Darwis, Dedi, A. Ferico Pasaribu, and Ade Surahman. (2019). "Sistem Pencarian Lokasi Bengkel Mobil Resmi Menggunakan Teknik Pengolahan Suara Dan Pemrosesan Bahasa Alami." *Jurnal Teknoinfo* 13(2):71–77.

Darwis., D., Kisworo., 2017, Teknik steganografi untuk penyebunyian pesan teks menggunakan algoritma end of file, Program Studi Manajemen Informatika , AMIK Teknokrat Lampung, Kedaton, Bandarlampung.

Djuwitaningrum., E., R., Apriyani., M., 2016, "*Text Message Steganography Using Least Significant Bit Method and Linear Congruential Generator Algorithm"*, Program Studi Informatika , Institut Teknologi Indonesia, Serpong, Tangerang Selatan.

Endang, R., D., Melis, A., 2016,"*Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator*" JUITA ISSN: 2086-9398 Vol. IV Nomor 2, November 2016 Institut Teknologi Indonesia Jl. Raya Puspiptek, Serpong, Tangerang Selatan.

Isnain, Auliya Rahman, Adam Indra Sakti, Debby Alita, and Nurman Satya Marga. 2021. "SENTIMEN ANALISIS PUBLIK TERHADAP KEBIJAKAN LOCKDOWN PEMERINTAH JAKARTA

MENGGUNAKAN ALGORITMA SVM." *Jurnal Data Mining Dan Sistem Informasi* 2(1):31–37.

Laudhana, Andre Chandra, Ajeng Savitri Puspaningrum, and Universitas Teknokrat Indonesia. 2020. "MEDIA PEMBELAJARAN TENSES UNTUK ANAK SEKOLAH MENENGAH PERTAMA BERBASIS ANDROID MENGGUNAKAN CONSTRUCT 2." 1(1).

Maulida, Sufia, Fikri Hamidy, and Agung Deni Wahyudi. 2020. "Monitoring Aplikasi Menggunakan Dashboard Untuk Sistem Informasi Akuntansi Pembelian Dan Penjualan (Studi Kasus: UD Apung)." *Jurnal Tekno Kompak* 14(1).

Megawaty, Dyah Ayu, Setiawansyah, Muhammad Bakri, and Evi Damayanti. 2020. "SISTEM MONITORING KEGIATAN AKADEMIK SISWA." 14(2):98–101.

Mishra, Minati, and Priyadarsini Mishra. 2012. "Digital Image Data Hinding Techniques." *ANSVESA* 7(2):105–15.

Pal, Ak, and Tarok Pramanik. 2013. "Design of an Edge Detection Based Image Steganography with High Embedding Capacity." *Quality, Reliability, Security and Robustness in …* 794–800.

Paraskevov, Hristo , Zhelezov, Stanimir Boryana, Uzunova,D.,2017,"*Robustness of the secret message in stego file against flip and rotaion attack*", Faculty of Mathematics and Computer Science, Shumen University, Shumen, Bulgaria.

Qilin Qi, Aaron,S., Dongming, P.,, Yaoqing, Y., and Hamid, S., 2016 ,"*Generic attack against robust steganography based on spring transform and geometrization*", Security and Communcation Network, Department of Electrical and Computer Engineering, University of Nebraska–Lincoln, Lincoln, NE, U.S.A.

Putra, Ade Dwi. 2020. "RANCANG BANGUN APLIKASI E-COMMERCE UNTUK USAHA PENJUALAN HELM." *Jurnal Informatika Dan Rekayasa Perangkat Lunak* 1(1):17–24.

Rahmanto, Yuri, Muhammad Farhan Randhika, Faruk Ulum, and Bentar Priyopradono. 2020. "APLIKASI PEMBELAJARAN AUDIT SISTEM INFORMASI." 14(2):62–67.

Shashikala,. C, Ajay, J., 2009, "*Steganography An Art of Hiding Data*", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

Silverstein, D. A., and J. E. Farrell. 1996. "The Relationship between Image Fidelity and Image Quality." *IEEE* 1:881–84.

Suaidah, Suaidah, and Irvan Sidni. 2018. "Perancangan Monitoring Prestasi Akademik Dan Aktivitas Siswa Menggunakan Pendekatan Key Performance Indicator (Studi Kasus SMA N 1 Kalirejo)." *Jurnal Tekno Kompak* 12(2):62–67.

Sulistiani, Heni, Retno Triana, and Neneng Neneng. 2018. "Sistem Informasi Akuntansi Pengelolaan Piutang Usaha Untuk Menyajikan Pernyataan Piutang (Open Item Statement) Pada PT Chandra Putra Globalindo." *Jurnal Tekno Kompak* 12(2):34.

Ujianto, E.I.H., A,. Harjoko, R., Wardoyo, A., Moesirami,2015, "*Cascaded Image Steganography to Incrace Robustness agaist attack of the Stego Image*", Journal of Theoretical and Applied Information Technology 30th September 2015. Vol.79. No.3.

Wantoro, Agus. 2021. "Sistem Monitoring Perawatan Dan Perbaikan Fasilitas Gardu PT PLN Area Kota Metro." *Jurnal Tekno Kompak* 15(1):116–30.

Wantoro, Agus, and Adhie Thyo Priandika. 2017. "STATISTIK KLASIK DENGAN LOGIKA FUZZY (TSUKAMOTO DAN MAMDANI) STUDI KASUS : STMIK."