Penerapan Pembangkit Bilangan Acak dalam Steganografi

Bayu Samudra - 13520128[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13520128@std.stei.itb.ac.id

***Abstrak*—Steganografi adalah ilmu yang mempelajari cara untuk menyembunyikan data. Steganografi memiliki banyak cara, salah satunya adalah menggunakan metode LSB dengan penempatan acak. Penempatan dilakukan berdasarkan hasil yang dikeluarkan oleh pembangkit bilangan acak LCG. Kelebihan dari penggunaan ini adalah mudahnya dalam implementasi, data yang disimpan lebih tersamarkan saat pengujian menggunakan steganalisis visual, dan adanya sebuah kunci pengaman data yang disimpan melalui umpan dari pembangkit bilangan acak. Kelamahan dari metode ini adalah data yang disimpan sangat mudah rusak, mudah terdeteksi dengan melakukan steganalisis statistik, mudahnya kunci ditemukan dengan menggunakan *brute-force*.**

***Kata Kunci*—Keamanan, Steganografi, *Linear Congruetial Generator* (LCG)**

I. Pendahuluan

Dunia saat ini telah memasuki era yang penuh dengan data. Data setiap waktunya bertumbuh secara ekponensial. Data merupakan hal yang sangat penting bagi setiap orang. Data yang tersebar pada internet banyak jenisnya. Ada data yang merupakan data yang memang dibagikan untuk publik bahkan ada juga sata rahasia yang bersifat privat. Data yang bersifat privat ini haruslah dijaga kerahasiaannya. Sealh satu cara untuk menjaganya adalah dengan menggunakan kriptografi.

Kriptografi adalah ilmu yang mempelajari mengenai cara-cara untuk menjaga integritas dan keamanan dari suatu data. [1] Dalam menjaga data, kriptografi menggunakan cabang-cabang ilmu matematika terutama dalam teori bilangan. Kriptografi juga merupakan sebuah seni. Hal ini dikarenakan pada awal kemunculannya, setiap orang memiliki caranya tersendiri untuk mengamankan pesannya. Terdapat banyak kriptografi klasik seperti Caesar Cipher, Vigenere Cipher, Affine Cipher, dan lainnya.

Selain menggunakan kriptografi, terdapat sebuah teknik lain untuk mengamankan sebuah data. Teknik ini dikenal steganografi. Steganografi adalah sebuah ilmu yang mempelajari teknik-teknik bagaimana menyembunyikan sebuah data dalam sebuah media sehingga sulit untuk dikenali. Steganografi ini sudah dikenal cukup lama sejak sejak bangsa Yunani. Steganografi yang pernah tercatat pada zaman itu adalah saat penguasa bernama Histaiaeus, seorang penguasa Yunani, mengirimkan pesan tersembunyi kepada Aristagoras untuk melawan Persia. Sang penguasa mengirimkan pesan tersebut dengan membotaki para budah dan rambutnya dibiarkan tumbuh, lalu dikirimkanlah kepada Aristagoras. Hal ini dapat dilihat pada buku yang telah ditulis oleh Herodatus, *Histories of Herodatus*. [1]

Steganografi ini berbeda dengan Kriptografi. Pada kriptografi, data diubah menjadi sesuatu yang sulit dipahami makna pesan yang ada didalamnya. Akan tetapi, data tersebut masih ada keberadaanya. Dalam Steganografi, data disembunyikan dalam sebuah medium sehingga tidak terlihat keberadaannya. Medium ini bisa apapun, baik itu gambar, video, file, atau bahkan teks. Data pada medium ini pada akhirnya harus bisa diekstraksi untuk diambil pesannya.

Steganografi ini memiliki kelebihan, yaitu data yang dikirimkan tidak menarik perhatian orang lain. Steganografi ini pun dapat diintegrasikan dengan Kriptografi untuk meningkatkan keamanan data yang disimpan.

II. Teori Dasar

A. Terminologi Dasar Steganografi

Dalam Steganografi, dikenal beberapa terminologi dasar. Berikut ini adalah beberapa terminologi dasar yang perlu diketahui: [1]

- Pesan tersembunyi adalah pesan yang disisipkan pada sebuah medium baik itu berupa video, image, audio, ataupun teks.
- Cover adalah media yang digunakan untuk menyisipkan pesan.
- *Stegeo-object* adalah media yang telah tersisipkan pesan tersembunyi di dalamnya.
- Steganalisis adalah cabang ilmu yang membahas mengenai pendeteksian pesan tersembunyi yang ada pada sebuah media. Terdapat beberapa jenis metode dalam steganalisis ini yang akan dijelaskan pada bagian selanjutnya.

B. Kriteria Kualitas Steganografi

Sebuah steganografi dikatakan memiliki kualitas yang baik apabila mengikuti beberapa kriteria berikut: [1]

- *Impercepibility* yaitu perubahan oleh steganografi tidak boleh dapat dirasakan oleh inderawi. Hal ini ditujukan agar tidak menimbulkan kecurigaan orang lain.
- *Fidelity* yaitu perubahan oleh steganografi tidak jauh mengurangi kualitas dari suatu cover. Misalkan pada

cover gambar, steganografi tidak boleh membuat gambar tersebut menjadi pecah.
- *Recovery* yaitu pesan yang disisipkan oleh proses steganografi haruslah bisa diekstraksi kembali.
- *Payload* yaitu pesan yang disisipkan dapat dimuat sebanyak mungkin.
- *Robustness* yaitu *stegeo-object* harus tahan terhasap serangan padanya. Akan tetapi, aspek in tidak terlalu dipentingkan karena steeganografi menyembunyikan pesan sehingga tidak menimbulkan kecurigaan.

C. Jenis Steganalisis

Steganalisis terbagi menjadi beberapa jenis. Berdasarkan kespesifikannya, steganalisis dibagi menjadi dua jenis, yaitu sebagai berikut [1]

- *Targeted Steganalysis* yaitu steganalisis yang membatasi analisis pada media atau algoritma steganografi tertentu.
- *Blind Steganalysis* yaitu steganalisis yang menganalisis dari berbagai algoritma dan format media. Hasil statistik dar setiap data akan dibandingkan dan diambil kesimpulan.

Selain berdasarkan kespesifikannya, steganografi juga dibagi menjadi menjadi dua berdasarkan metode yang digunakan.

- *Visual Steganalysis* yaitu steganalisis yang dilakukan dengan indera visual. Steganalisis jenis ini bersifat sujektif.
- *Statistical Steganalysis* yaitu steganalisis yang menganalisis menggunakan analisis matematika terutama menggunakan statistika.

D. Representasi Bilangan Bulat

Pada dasarnya, komputer menyimpan dan memproses informasi dalam bentuk sinyal duanilai. Setiap sinyal tersebut merepresentasikan angka dalam bentuk bit. Kumpulan dari berbagai bit dapat memberikan makna dari suatu data yang sedang diproses. Kumpulan dari berbagai bit ini dapat membantuk sebuah bilangan yang disebut dengan bilangan biner.

Dalam dunia keinformatikaan, terdapat dua jenis representasi bilangan bulat yang sering digunakan yaitu sebagai berikut:

- **Bilangan Biner**
  Bilangan biner yaitu bilangan dengan basis dua. Bilangan biner hanya terdapat dua simbol yang tersedia, yaitu 0 dan 1. Konversi bilangan biner ke bilangan desimal didefinisikan pada persamaan 1.

$$d = \sum_{i=0}^{n} b_i \cdot 2^i \tag{1}$$

  Nilai b_i melambangkan digit biner ke-i dan d adalah bilangan desimal hasil konversi.

- **Bilangan Hexadesimal**
  Bilangan Hexadesimal adalah bilangan dengan basis 16. Dua digit dari bilangan ini merepresentasikan satu byte (8-bit). Bilangan Hexadesimal ini dapat meringkas penulisan biner dan juga memudahkan alam penganalisisan bilangan biner. Bilangan hexadesimal ini pada dasarnya terdiri dari simbol 0 sampai dengan 9 dilanjutkan dengan simbol A,B,C,D,E, dan F. Berikut ini adalah rumus konversi bilangan heksadesimal ke bilangan desimal.

$$d = \sum_{i=0}^{n} h_i \cdot 16^i \tag{2}$$

  Nilai h_i menyatakan digit hexadesimal ke-i. Bila digit Hexadesimal bernilai A maka digantikan dengan nilai 10. Begitu pula dengan nilai B yang digantikan dengan nilai 11. Hal ini berlaku seterusnya hingga F.

E. Signifikansi Bit

Terdapat dua buah definisi yang perlu diperhatikan mengenai signifikansi bit.Misalkan terdapat sebuah bilangan bulat dengan w-digit dan urutan digitnya adalah $[b_{w-1}, b_{w-2}, \cdots, b_2, b_1, b_0]$. Digit b_{w-1} disebut sebagai *most significant bit* atau biasa disingkat sebagai MSB. Bit b_0 disebut sebagai *least significant bit* atau biasa disingkat sebagai LSB.

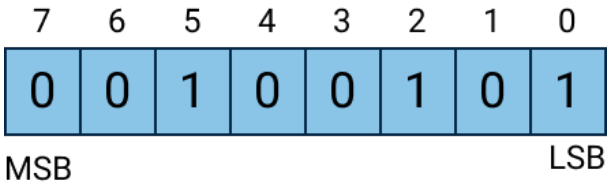

Fig. 1. Ilustrasi MSB dan LSB

F. Citra Digital

Pada komputer sebuah citra digital disimpan dalam kumpulan byte data. Bagian terkecil dari sebuah citra digital disebut dengan pixel. Citra digital merupakan matriks dari pixel tersebut. Setiap pixel direpresentasikan dengan bilangan n-bit. Berdasarkan jumlah bit pada pixel, citra digital dapat diklasifikasikan menjadi beberapa jenis yaitu sebagai berikut: [1] [3]

- **Citra 24-bit**
  Pada citra 24-bit, setiap pixel terdiri atas 3 buah kanal. Kanal pada citra ini adalah yaitu R (*Red*), G (*Green*), dan B (*Blue*). Setiap kanal memiliki besar 8-bit yang merepresentasikan bilangan 0 sampai 255.
- **Citra 8-bit**
  Citra ini biasa disebut sebagai citra grayscale. Citra ini hanya memiliki 1 buah kanal yang menyatakan nilai keabuan. Konversi dari citra berwarna menjadi citra grayscale ini dapat dilakukan dengan rumus pada persamaan 3.

$$y = 0.299 \cdot R + 0.587 \cdot G + 0.144 \cdot B \tag{3}$$

  Citra pada figur 3 adalah hasil konversi citra pada figur 2 menjadi grayscale.

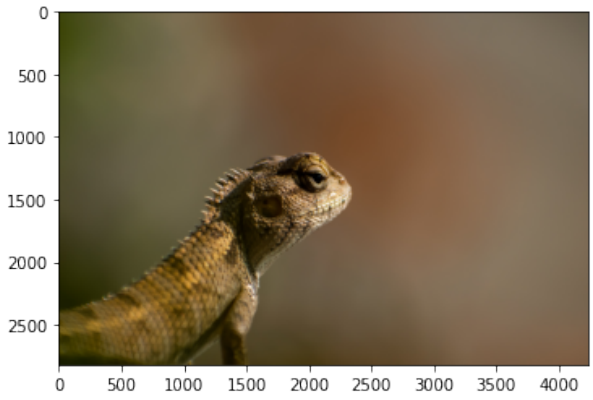

Fig. 2. Citra berwarna 24-bit (Sumber: Unsplash)

Fig. 3. Citra berwarna 8-bit)

- **Citra 1-bit**
  Citra 1-bit ini biasa dikenal dengan citra biner. Citra ini hanya memiliki dua kemungkinan nilai pixel, yaitu 0 atau 1. Jenis citra ini biasa digunakan sebagai *masking* dalam pengolahan citra. Citra pada figur 4 adalah hasil konversi pada citra figur 2 menjadi citra biner.

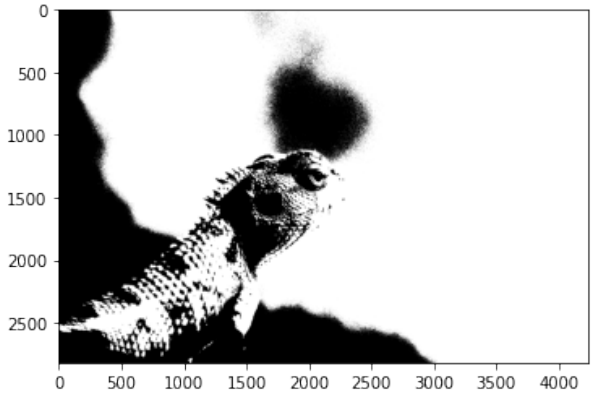

Fig. 4. Citra berwarna 1-bit

G. *Luminans Relatif*

Tingkat Luminans Relatif sebuah warna ini dapat dihitung menggunakan persamaan 4. [6]

$$L = 0.2126R_p + 0.7152G_p + 0.0722B_p \tag{4}$$

yang dalam hal ini

$$X_p = \begin{cases} \frac{X_r}{12.92}, & \text{jika } X_r \leq 0.03928 \\ (\frac{X_r+0.055}{1.055})^{2.4}, & \text{jika } X_r > 0.03928 \end{cases}$$

dengan X adalah salah satu dari R, G, ataupun B.

Nilai dari X_r merupakan rasio suatu kanal warna terhadap nilai maksimumnya.

H. *Rasio Kontras*

Rasio kontras antara dua buah warna menyatakan seberapa kontras kedua warna tersebut. Menurut W3C, tingkat rasio kontras didefinisikan pada persamaan 5. [6]

$$R = \frac{L_1 + 0.05}{L_2 + 0.05} \tag{5}$$

yang dalam hal ini L_n adalah luminans relatif dari satu warna dengan $L_1 > L_2$.

I. *Keterbagian Bilangan Bulat*

Pembagian merupakan konsep penting yang menjadi dasar dari teori bilangan. Sebuah bilangan dapat membagi habis bilangan lain. Definisi dari habis dibagi dapat dilihat pada definisi II.1.

Definisi II.1. Misalkan x dan y adalah sebuah bilangan bulat. Dapat dikatakan x habis membagi y atau dinotasikan dengan

$$a|b$$

jika dan hanya jika terdapat sebuah bilangan bulat a yang memenuhi persamaan $y = ax$

Dalam berbagai bilangan bulat, terdapat satu kelompok bilangan bulat yang sangat penting yaitu bilangan prima.

Definisi II.2. Sebuah bilangan bulat x dengan $x > 0$ dikatakan bilangan prima jika dan hanya jika bilangan tersebut hanyalah habis dibagi oleh x dan 1.

Terdapat teorema penting mengenai bilangan prima yang disebut dengan teorema fundramental aritmatik. [2]

Teorema II.1 (Teorema Fundramental Aritmatik)**.** Setiap bilangan bulat positif yang lebih dari sama dengan 2 dapat dinyatakan sebagai perkalian yang setidaknya terdapat sebuah bilangan prima.

Setiap bilangan prima yang dapat membagi sebuah bilangan bulat disebut dengan faktor prima.

J. Aritmatika Modulo

Dalam teori bilangan dikenal sebuah operasi yang disebut dengan operasi aritmatika modulo. Aritmatika modulo ini memainkan peran penting dalam Kriptografi untuk membantu mengamankan data. Operator yang digunakan pada operasi modulo adalah mod. Operasi ini didefinisikan pada definisi II.3.

Definisi II.3. Misalkan x dan m adalah sebuah bilangan bulat dengan $m > 0$. Kesamaan $x \mod m = r$ merupakan kesamaan semedikian sehingga $x = ma + r$ dengan nilai $0 \leq r < m$. Dengan kata lain, r adalah sisa bagi dari pembagian x dan m.

Dalam aritmatika modulo, terkadang dua buah bilangan bisa saja memiliki hasil modulo yang sama. Kedua bilangan ini bisa disebut kongruen dalam suatu modulo. Kekongruenan ini dapat didefinisikan sebagaimana definisi II.4.

Definisi II.4. Misalkan terdapat tiga buah bilangan bulat a, b, dan m dengan $m > 0$. Dapat dikatakan bahwa bilangan a dan b kongruen atau dengan notasi

$$a \equiv b \pmod{m}$$

jika dan hanya jika $a - b$ habis dibagi oleh m.

K. Pembagi Bersama Terbesar

Dua buah bilangan bulat bisa saja habis dibagi dengan suatu bilangan bulat. Pembagi ini bisa saja lebih dari satu. Akan tetapi, terdapat sebuah bilangan pembagi dari kedua buah bilangan bulat tersebut yang disebut dengan pembagi bersama terbesar (PBB) atau disebut dengan *greatest common divisor* (GCD).

Definisi II.5. Misalkan terdapat dua buah bilangan bulat a dan b dengan $a, b > 0$. Dikatakan x merupakan $\gcd(a, b)$ jika dan hanya jika x bilangan bulat terbesar yang memenuhi $x|a$ dan $x|b$.

Terdapat sebuah istilah yang cukup penting, yaitu relatif prima. Dua buah bilangan bisa dikatakan relatif prima bila memenuhi definisi II.6.

Definisi II.6. Misalkan terdapat dua buah bilangan bulat a dan b dengan $a, b > 0$. Dikatakan a relatif prima dengan b jika dan hanya jika $\gcd(a, b) = 1$.

L. Pembangkit Bilangan Acak

Dalam dunia keinformatikaan, bilangan acak merupakan bilangan yang sangat dibutuhkan. Bilangan acak sangat diperlukan terutama dalam kriptografi. Terdapat berbagai jenis pembangkit bilangan acak, salah satunya adalah *Linear Congruential Generator* (LCG). Bilangan acak ini didefinisikan dalam relasi rekurens pada persamaan 6.

$$x_{i+1} = ax_i + b \pmod{m} \tag{6}$$

Untuk memulai LCG, diperlukan sebuah umpan yaitu x_0. Dengan umpan yang sama, dapat didapatkan sebuah nilai urutan yang sama. Parameter a, b dan m sangat menentukan periode dari LCG. Terdapat sebuah teorema yang dapat membantu menentukan nilai a, b, dan m agar memperoleh periode maksimum. [5]

Teorema II.2 (Teorema Hull–Dobell)**.** Sebuah LCG yang didefinisikan pada definisi 6 dapat memiliki periode penuh, yaitu berperiode $m - 1$ jika memenuhi syarat berikut:

1) b relatif prima terhadap m,
2) $a \equiv 1 (\mod p)$ jika p merupakan faktor prima dari m,
3) $a \equiv 1 (\mod 4)$ jika m adalah bilangan yang habis dibagi oleh 4.

III. Pembahasan

A. Metode Steganografi

Pada penelitian ini, akan digunakan metode steganografi berbasis LSB. Nilai m yang digunakan adalah jumlah pixel yang terdapat pada cover. Metode penyisipan yang digunakan adalah sebgai berikut.

1) Menentukan parameter a dan b untuk LCG.
2) Mengubah gambar menjadi dalam bentuk matriks pixel.
3) Mengubah matriks pixel menjadi array lanjar agar lebih mudah untuk diolah.
4) Menentukan angka acak dengan menggunakan LCG.
5) Mengambil n bit dari lsb dari data yang akan disisipkan, lalu menimpa pada array lanjar.
6) Kembali melakukan dimulai dari langkah 4 hingga semua data yang akan disisipkan sudah dimasukan atau tidak tersedia ruang untuk menambahkan data baru.
7) Menambahkan string `"\x00"` pada array lanjar dengan menggunakan angka acak selanjutnya. Langkah ini dilakukan apabila ruang untuk memasukan data ini masih tersedia.

Langkah yang dilakukan untuk mengekstraksi data pada *stegeo-object* adalah sebagai berikut:

1) Menentukan parameter a dan b untuk LCG.
2) Mengubah gambar menjadi dalam bentuk matriks pixel.
3) Mengubah matriks pixel menjadi array lanjar agar lebih mudah untuk diolah.
4) Menentukan angka acak dengan menggunakan LCG.
5) Mengambil n bit dari lsb array lanjar pada indeks yang ditunjukan oleh hasil LCG. Kumpulkan hingga mendapatkan 8-bit. Pengumpulan menggunakan aturan little endian.
6) Bila telah mencapai 8-bit, ubahlah bit yang telah dikumpulkan menjadi karakter.
7) Lakukan kembali dimulai langkah 4 hingga didapatkan 1 byte yang bernilai 0. Hasil itu menjadi penanda bahwa proses telah berakhir.

Jumlah n yang disarankan untuk melakukan proses ini adalah n yang memenuhi $n = 2^k$ dengan k adalah bilangan bulan dan $k \leq 8$. Hal ini dilakukan agar mendapatkan kelipatan 8 setiap iterasi saat melakukan ekstraksi pesan.

```
def get_lowest_multiplier(m):
  """Menentukan nilai a"""
  isDiv4 = (m % 4 == 0)
  i = 2
  factorMultiply = 1

  while i * i <= m:
    if m % i:
      i += 1
    else:
      m //= i
      factorMultiply *= i

      while m % i == 0:
        m //= i

  if m > 1:
    factorMultiply *= m

  if isDiv4:
    factorMultiply <<= 1

  return factorMultiply + 1

def get_b(m):
  num = 1

  while m % num == 0:
    num = random.randint(2,m)

  return num
```

Fig. 5. Algoritma Penentuan nilai parameter a dan b

B. Pemilihan Parameter

Pemilihan parameter a dilakukan dengan cara menentukan semua faktor prima dari m. Semua faktor prima dikalikan dan didapatkanlah nilai $a-1$. Dengan kata lain, persamaan 7 adalah persamaan yang digunakan untuk mencari nilai a yang ideal.

$$a = 1 + \prod_{i \in p} i, \ p \text{ adalah faktor prima dari } m \tag{7}$$

Apabila m habis dibagi oleh 4, maka hasil perkalian dikalikan kembali dengan 2 agar menjaga nilai m selalu memenuhi teorema II.2. Persamaan 8 merupakan kasus khusus m yang dapat dibagi oleh 4.

$$a = 1 + 2\prod_{i \in p} i, \ p \text{ adalah faktor prima dari } m \tag{8}$$

Algoritma pada figur 5 merupakan algoritma yang dapat digunakan untuk menentukan nilai diatas.

Penentuan parameter dengan algoritma diatas dijamin untuk memberikan nilai bilangan acak yang relatif lebih merata dan juga memiliki periode yang panjang.

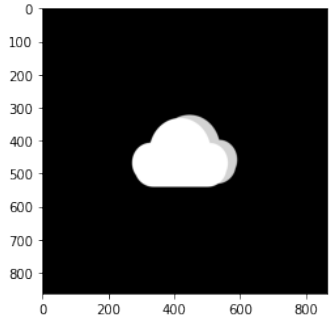

Fig. 6. Cover grayscale yang digunakan untuk dilakukan steganografi

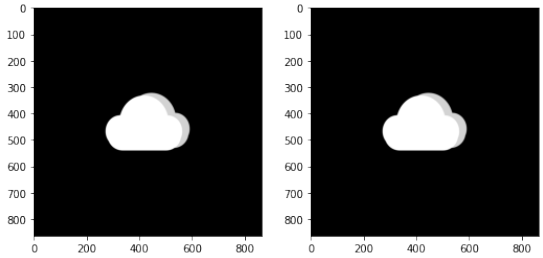

Fig. 7. Stegano-object hasil dari penyisipan data pada gambar figur 6. Gambar kiri merupakan hasil dengan tanpa pengacakan dan kanan merupakan hasil dengan pengacakan

C. Perbandingan Steganalisis Dengan Pengacakan dan Tanpa Pengacakan

Pada bagian ini, akan dicoba untuk menganalisis dampak dari pengacakan data yang dimasukan pada cover dengan tanpa dilakukannya pengacakan. Gambar yang akan digunakan adalah gambar grayscale yang ditunjukan oleh figur 6.

Cover pada figur 6 akan disisipi pesan sebanyak 5000 karakter dengan jumlah bit $n = 1$. Hasil pada figure 7 yang didapatkan setelah melakukan steganografi secara acak dan tidak acak.

Pada *stego-object* tersebut tidak ditemukan perubahan yang signifikan pada cover. Akan tetapi, penempatan ini akan sangat berpengaruh pada saat melakukan steganalisis. Steganalisis dilakukan dengan cara mengubah semua bit pada pixel menjadi bit lsb. Hal ini menimbulkan hasil pada figur 8.

Bila dilihat secara lebih detail, gambar kiri menyisakan

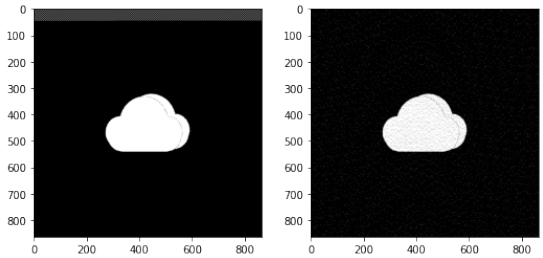

Fig. 8. Hasil steganalisis figur 7. Gambar kiri merupakan hasil dengan tanpa pengacakan dan kanan merupakan hasil dengan pengacakan

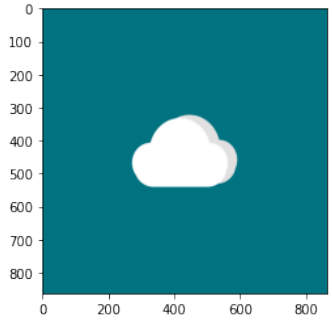

Fig. 9. Cover berwarna akan digunakan dalam steganografi

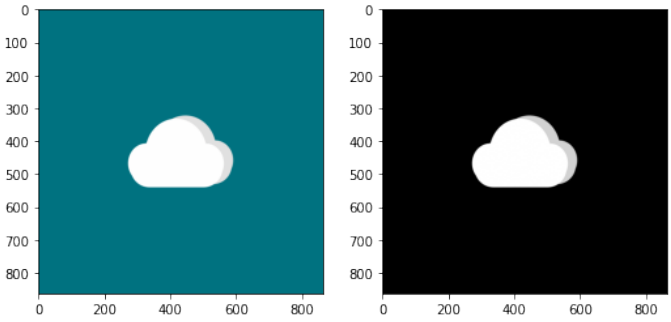

Fig. 10. Hasil steganografi gambar pada dua buah media

sekumpulan warna abu-abu pada awal hasil steganalisis. Akan tetapi pada gambar kanan, tidak begitu terlihat adanya perubahan pada hasil steganalisis. Hal ini disebabkan karena pengacakan membuat data tidak berada posisi yang cukup berjauhan. Oleh karena itu, pengacakan membuat proses steganalisis lebih sulit dibandingkan dengan tanpa adanya pengacakan.

D. Perbandingan Steganalisis Pada Cover Grayscale dan Berwarna

Pada bagian ini, akan dilakukan percobaan dengan melakukan proses steganalis pada media berwarna dan media grayscale. Media berwarna yang digunakan pada proses ini adalah figur 9 dan cover yang digunakan untuk media grayscale adalah figur 6. Data yang akan disisipkan sebanyak 75.000 data. Pengaturan untuk konstanta a diberikan nilai yang sama sebagaimana pada subbab sebelumnya.

Hasil steganografi yang didapatkan untuk media berwarna dan grayscale ditunjukan pada figur 10.

Steganalisis yang dilakukan serupa degan steganalisis yang dilakukan pada subbab sebelumnya. Hasil dari steganalisis untuk gambar asli baik itu grayscale ditunjukan oleh figur 11 dan steganalisis untuk gambar berwarna asli ditunjukan oleh 12.

Hasil steganalisis pada *stegeo-object* berwarna ditunjukan pada figur 13, sedangkan untuk media grayscale ditunjukan pada figur 14.

Dari hasil steganalisis pada figur 13 terlihat terapat banyak sekali *noise* yang muncul pada hasil steganalisis visual. Pada hasil steganalisis pada figur 14 terlihat bahwa *noise* yang

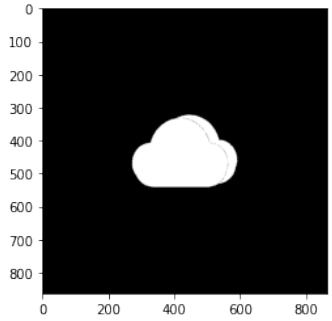

Fig. 11. Hasil steganalisis gambar grayscale asli

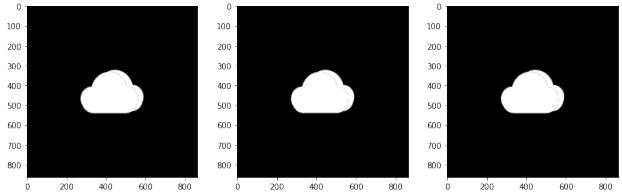

Fig. 12. Hasil steganalisis gambar berwarna asli. Dimulai dari kiri hingga kanan berturut-turut menyatakan kanal R,G,dan B

muncul lebih merata kepada tiap-tiap channel warna. Hal ini menunjukan bahwa tiap data disisipkan secara menyebar pada cover berwarna untuk setiap kanal. Hal ini tentu memberikan dampak baik karena data yang dimasukan akan lebih tersamarkan jika menganalisis menggunakan steganografi visual.

Keuntungan penggunaan kanal berwarna, cover memberikan lebih banyak ruang yang dapat disimpan pada gambar. Pada gambar dengan pixel 24-bit akan memberikan ruang 3 kali lebih besar daripada menggunakan grayscale. Penambahan ruang juga dapat dicapai dengan menggunakan lebih dari satu bit LSB dari gambar.

E. Kelebihan dan Kekurangan Sistem Steganografi Metode LSB Acak

Sistem steganografi dengan metode LSB Acak memiliki keuntungan yaitu kemudahannya dalam implementasi. Sistem steganografi ini juga secara kasat menghasilkan *stegeo-object* yang sulit untuk dibedakan dengan gambar yang asli. Hal ini

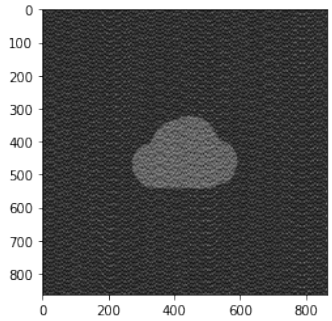

Fig. 13. Hasil steganalisis dari *stegeo-object* dengan cover grayscale

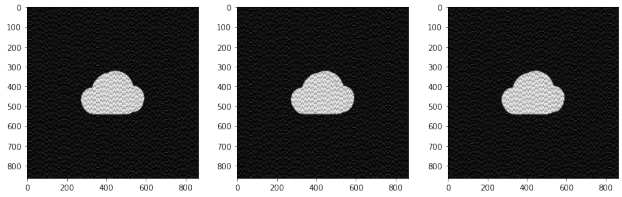

Fig. 14. Hasil steganalisis dari *stegeo-object* dengan cover grayscale. Dimulai dari kiri secara berturut-turut menyatakan kanal warna R,G,dan B

dikarenakan setiap pixel warna berubah tidak jauh dari hasil asli sehingga perubahan antara keduanya dapat tersembunyikan. Sistem ini juga dapat diintegrasikan dengan kriptografi agar menjaga data lebih aman lagi dari sebelumnya. Pemilihan seed yang acak memiliki keuntungan yaitu menjadi kunci dari *stegeo-object*.

Kekurangan dari steganografi ini adalah data yang disimpan sangat rentan terhadap perubahan kecil. Salah satu perubahan yang dapat merusak steganografi ini adalah proses kompresi gambar. Selain itu, kunci berbasis seed sangat mudah sekali untuk dicari dengan melakukan *brute-force* pada *stegeo-object*. Sistem steganografi ini sangat lemah terhadap steganalisis statistik karena perubahan yang terjadi pada setiap proses akan memberikan dampak yang besar pada hasil statistik.

IV. Kesimpulan

Steganografi merupakan salah satu cara untuk menyembunyikan data pada sebuah cover. Steganografi memiliki banyak cara, salah satunya adalah steganografi dengan metode LSB. Metode LSB ini sangatlah sederhana dan mudah untuk diimplementasikan pada sebuah media baik itu gambar maupun media lainnya.

Penggunaan sistem acak dan penggunaan multi kanal dapat meningkatkan kualitas dari steganografi yang dilakukan. hal ini ditunjukan dengan hasill steganalisis visual yang menunjukan sistem acak memberikan keamanan lebih dibandingkan tanpa pengacakan. Selain itu, penggunaan kanal secara merata dapat juga memberikan penyamaran lebih terhadap steganalisis visual sehingga lebih sulit dikenali.

Ucapan Terima Kasih

Alhamdulillah, segala puji Allah SWT karena atas pertolongan dan rahmatnya, saya dapat menyelesaikan makalah ini. Penulis juga turut memberikan ucapan terima kasih kepada keluarga yang selalu setia untuk memberikan motivasi dan semangat untuk dapat menyelesaikan makalah ini. Penulis juga turut mengucapkan terima kasih kepada para dosen pengampu mata kuliah Matematika Diskrit, yaitu ibu Dr. Nur Ulfa Maulidevi, S.T., M.Sc., bapak Dr. Ir. Rinaldi Munir, M.T., dan ibu Dra. Harlili S., M.Sc. atas segala ilmunya yang telah membantu penulis dalam menyelesaikan makalah ini. Semoga dengan kebaikan yang telah diberikan, Allah akan menggantinya dengan yang lebih baik lagi.

Sumber Daya

Segala sumber daya yang digunakan untuk membangun makalah ini dapat anda akses pada https://github.com/bayusamudra5502/Matdis-Steganografi.

Daftar Pustaka

[1] Munir, Rinaldi. 2019. *Kriptografi Edisi Kedua*. Bandung: Penerbit Informatika

[2] Munir, RInaldi. 2020. *Matematika Diskrit Revisi Ketujuh*. Bandung: Penerbit Informatika

[3] HIdayatullah, Priyanto. 2017. *Pengolahan Citra Digital Teori dan Aplikasi Nyata*. Bandung: Penerbit Informatika.

[4] Briant, Randal E. & O'Hallaron, David R. 2016. *Computer System A Programmer's Perspective Third Global Edition*. London: Pearson Education.

[5] Hull, T. E. & Dobell, A. R. 1962. Random Number Generators. SIAM Review, 4(3), 233. Diakses pada 2021-12-04 melalui http://chagall.med.cornell.edu/BioinfoCourse/PDFs/Lecture4 /random_number_generator.pdf.

[6] Konsorsium World Wide Web. 2008. Web Content Accessibility Guidelines (WCAG) 2.0. Web content accessibility guidelines (WCAG) 2.0. Diakses 2021-12-04 melalui https://www.w3.org/TR/2008/REC-WCAG20-20081211/.

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis adalah tulisan saya sendiri, bukan sanduran, ataupun terjemahan dari makalah orang lain, dan bukan plagiasi.

Cimahi, 14 Desember 2021

Bayu Samudra - 13520128