Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB

Muhamad Fitra Syawal[#1] , Deddy Chandra Fikriansyah[#2] , Nazori Agani[#3]

[#]*Program Studi Magister Ilmu Komputer, Universitas Budi Luhur*

Jl. Raya Ciledug, Jakarta Selatan, Indonesia (12260)

Telp. (021)5853753, Fax.(021)5853752

[1]1411600958@student.budiluhur.ac.id

[2]1411601022@student.budiluhur.ac.id

[3]nazori@budiluhur.ac.id

Abstrak **— Keamanan data dan informasi saat ini menjadi sebuah kebutuhan vital bagi para pengguna internet saat ini agar privasi mereka bisa tetap terjaga. Teknik pengamanan data yang saat ini banyak dipakai yaitu kriptografi dan steganografi. Kriptografi adalah teknik menyandikan (*enkripsi*) sebuah data rahasia menjadi data tersandi yang tidak dimengerti, sedangkan steganografi adalah teknik menyembunyikan pesan ke dalam sebuah media cover. Kelebihan steganografi daripada kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain, karena pesan-pesan tersebut dimasukan ke sebuah media penampung, sedangkan kriptografi hanya mengenkripsi pesan tersebut yang bisa saja menimbulkan kecurigaan orang lain.**

Kata Kunci **: Steganografi, Kriptografi, Vigenere Chiper, LSB**

Abstract **– Security Data and Information this day is urgent needed for internet user, for keep their privacy data. Many Data Secure Technique is used this day their are Cryptography and Steganography. Crypthography is encryption technique of secret data become encryption data can't understand by anyone. Steganography is hide technique text to cover media. Overplus from cryptography is this text not make attention anybody, because this text place to some contain media, and crypthography just encrypt the text which can make anybody suspicious.**

Keywords **: Steganografi, Kriptografi, Vigenere Chiper, LSB**

I. PENDAHULUAN

Seiring perkembangan zaman, kebutuhan manusia akan informasi semakin meningkat. Ditengah-tengah perkembangan teknologi informasi yang kian semarak, internet tidak lagi menjamin penyediaan informasi yang aman. Berbagai mesin-pencari (*search-engine*) terus berkembang ditambah dengan serangan *virus*, penyadap, *spam* maupun *hacker* yang menjamur dapat mencuri data-data bersifat rahasia. Mengatasi hal tersebut berbagai cara untuk meningkatkan keamanan data terus dikembangkan, diantaranya kriptografi dan steganografi.

Steganografi adalah seni dan ilmu menyembunyikan data pada media lain sebagai *cover* (misalnya citra) sehingga terlihat samar. Kriptografi adalah seni dan ilmu menjaga kerahasiaan data. Pada kriptografi, data asli diubah menjadi bentuk lain yang tidak dapat dibaca. Penggabungan steganografi dan kriptografi secara bersamaan dapat meningkatkan pengamanan data. Metode penggabungan steganografi dan kriptografi banyak dikembangkan. Pada umumnya teknik yang digunakan yaitu dengan mengenkripsi pesan terlebih dahulu (kriptografi), kemudian menyisipkannya ke media *cover* (steganografi). Namun, proses penyisipan dapat berpengaruh pada kualitas media *cover* tersebut.

Upaya untuk meminimalisir perubahan kualitas *cover* dapat dilakukan dengan penyisipan pada bit terakhir (*least significant bit*). Perubahan kualitas *cover* tidak tampak kasat mata, tetapi penyisipan pada bit terakhir dapat mengakibatkan pesan rusak ketia citra dikompresi. Ketahanan terhadap *robust* dapat dilakukan dengan pemilihan pada bit pertama (*most significant bit*), tetapi justru mengakibatkan perubahan kualitas *cover* menjadi tampak dan dapat dicurigai [1].

II. STEGANOGRAFI

A. SEJARAH STEGANOGRAFI

Teknik steganografi ini sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan *hieroglyphic* yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang

menggunakan gambar dianggap sebagai steganografi pertama di dunia [2]. Tidak hanya bangsa Mesir saja, bangsa-bangsa lain juga telah mengggunakan teknik steganografi pada masa lalu, yaitu :

1. Teknik steganografi yang lain adalah tinta yang tidak tampak (*invisible ink*) yaitu dengan menggunakan air sari buah jeruk, urin atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas api. Tinta yang sebelumnya tidak terlihat, ketika terkena panas akan menjadi gelap sehingga dapat dibaca. Teknik ini digunakan oleh bangsa Romawi yang juga digunakan pada Perang Dunia II.
2. Bangsa Cina menggunakan cara yang berbeda pula, yaitu manusia sebagai media pembawa pesan. Orang itu akan dicukur rambutnya sampai botak dan pesan akan dituliskan di kepalanya. Kemudian pesan akan dikirimkan ketika rambutnya sudah tumbuh.
3. Pada masyarakat Yunani kuno teknik yang digunakan adalah dengan menggunakan lilin sebagai media pembawa pesan. Lembaran pesan akan ditutup dengan lilin. Untuk melihat isi pesan, pihak penerima harus memanaskan lilin terlebih dahulu.
4. Pada Perang Dunia II, bangsa Jerman menggunakan *microdots* untuk berkomunikasi. Penggunaan teknik ini digunakan pada *microfilm chip* yang harus diperbesar sekitar 200 kali. Jerman menggunakan teknik ini untuk kebutuhan perang sehingga pesan rahasia strategi tidak diketahui pihak lawan. Karena pada saat itu teknik ini merupakan teknologi baru yang belum bisa digunakan lawan.

Akhir-akhir ini kata steganografi menjadi sering disebut di masyarakat bersama – sama dengan kata kriptografi setelah pemboman gedung WTC di AS, telah disebutkan oleh Pejabat Pemerintah dan Para Ahli dari Pemerintahan Amerika Serikat "yang tidak disebut namanya bahwa" bahwa Para Teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan web site lainnya. Walaupun demikian sebenarnya belum ada bukti nyata dari pernyataan-pernyataan tersebut diatas. Novel Da Vinci Code pun turut mempopulerkan steganografi dan kriptografi [3].

B. PENGERTIAN STEGANOGRAFI

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata *Steganos*, yang berarti tertutup dan *Graphia*, yang berarti menulis [4].

Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal [5].

Istilah steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama [2].

Steganografi adalah seni dan ilmu berkomunikasi dengan cara menyembunyikan keberadaan komunikasi itu. Berbeda dengan Kriptografi, di mana musuh diperbolehkan untuk mendeteksi, menangkal dan memodifikasi pesan tanpa bisa melanggar keamanan tempat tertentu yang dijamin oleh suatu *cryptosystem*, tujuan dari steganografi adalah untuk menyembunyikan pesan dalam pesan berbahaya lainnya dengan cara yang tidak memungkinkan musuh apapun bahkan untuk mendeteksi bahwa ada pesan kedua. Secara umum, teknik steganografi yang baik harus memiliki visual / *imperceptibility* statistik yang baik dan *payload* yang cukup [6].

C. TEKNIK *STEGANOGRAFI*

Menurut [2], ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu :

1. *Injection*, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut *embedding*.
2. *Substitusi*, data normal digantikan dengan data rahasia. Biasanya,hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada *file* media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
3 *Transform Domain*, teknik ini sangat efektif. Pada dasarnya,transformasi domain menyembunyikan data pada *transform space*. Akan sangat lebih efektif teknik ini diterapkan pada *file* berekstensi JPG.
4. *Spread Spectrum*, sebuah teknik pengtransmisian menggunakan *pseudo-noise code*, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
5. *Statistical Method*, teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. *Distortion*, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

7. *Cover Generation*, metode ini lebih unik daripada metode lainnya karena *cover object* dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah *Spam Mimic*.

D. PROSES STEGANOGRAFI

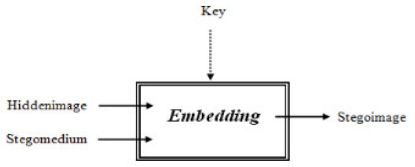
Secara umum, terdapat dua proses didalam steganografi. Yaitu proses *embedding* untuk menyembunyikan pesan dan ekstraksi untuk mengekstraksi pesan yang disembunyikan.

Gambar 1, menunjukkan proses penyembunyian pesan dimana di bagian pertama, dilakukan proses *embedding hiddenimage* yang hendak disembunyikan secara rahasia ke dalam *stegomedium* sebagai media penyimpanan, dengan memasukkan kunci tertentu (*key*), sehingga dihasilkan media dengan data tersembunyi di dalamnya (*stegoimage*).

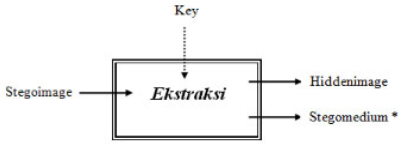
Pada Gambar 2, dilakukkan proses ekstraksi pada *stegoimage* dengan memasukkan *key* yang sama sehingga didapatkan kembali *hiddenimage*.

Kemudian dalam kebanyakan teknik steganografi, ekstraksi pesan tidak akan mengembalikan *stegomedium* awal persis sama dengan *stegomedium* setelah dilakukan ekstraksi bahkan sebagian besar mengalami kehilangan. Karena saat penyimpanan pesan tidak dilakukan pencatatan kondisi awal dari *stegomedium* yang digunakan untuk menyimpan pesan [4].

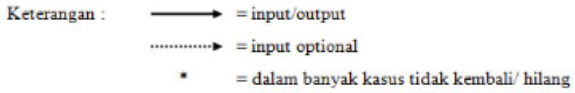
Berikut tampilan gambar 1 dan gambar 2 :



Gbr. 1 Embedding Citra



Gbr. 2 Ekstraksi Citra



III.. KRIPTOGRAFI

A. ALOGARITMA KRIPTOGRAFI KLASIK

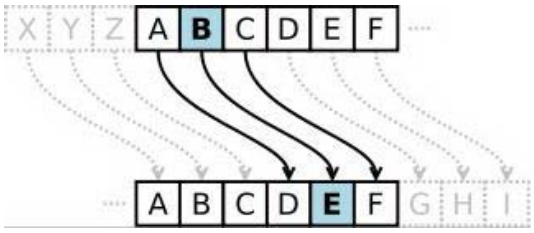
- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Algoritma kriptografi klasik:
  - *Cipher* Substitusi (*Substitution Ciphers*)
  - *Cipher* Transposisi (*Transposition Ciphers*)

B. *Chiper Substitusi*

- Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext
- Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext
- Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext
- Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext

C. *Chiper Substitusi – Caesar Cipher*

Merupakan sebuah metode yang sederhana, metode ini juga disebut sebagai substitusi kode yang pertama dalam dunia penyandian, karena penyandian ini terjadi pada saat pemerintahan Yulius Caesar. Dengan mengganti posisi huruf awal dengan alphabet atau disebut dengan algoritma ROT3 (penambahan 3).



Gbr.3 Proses penambahan pada algoritma ROT3

Teknik penyandian ini termasuk sandi tersubtitusi pada setiap huruf pada *plaintext* digantikan oleh huruf lain yang dimiliki selisih posisi tertentu dalam alphabet. Secara detail tabel 1 menjelaskan pergeseran yang terjadi pada huruf alphabet.

TABEL I.
ALPHABET SEBELUM PROSES PERGESERAN

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

TABEL II.
ALPHABET SETELAH PROSES PERGESERAN

D	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**
0	1	2	3	4	5	6	7	8	9	10	11	12
Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**A**	**B**	**C**
13	14	15	16	17	18	19	20	21	22	23	24	25

Jika pergeseran yang dilakukan sebanyak tiga kali, maka kunci untuk dekripsinya adalah 3. Pergeseran kunci yang dilakukan tergantung keinginan pengiriman pesan. Bisa saja kunci yang dipakai a = 7, b = 9, dan seterusnya.

Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet; alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet Biasa: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabet Sandi: DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut.

Contoh:

Plainteks : HAI TEMAN TEMAN
Cipherteks : *KDL WHPKQ WHPKQ*

- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:
  - *KDLW HPKQ WHPK Q*
- Atau membuang semua spasi:
  - *KDLWHPKQWHPKQ*
- Tujuannya agar kriptanalisis menjadi lebih sulit

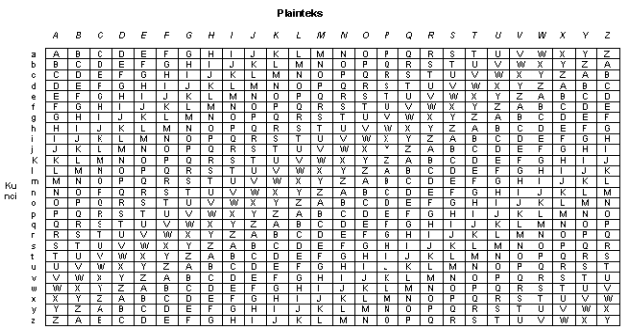
Proses Enkripsi dapat direpresentasikan menggunakan operator aritmatika *modullo* setelah sebelumnya setiap huruf transformasi ke dalam angka menggunakan ASCII *code*.

D. *Cipher Substitusi - Vigenere Cipher*

- Termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher).
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan Vigenere Cipher.
- Vigenere Cipher menggunakan Bujur sangkar Vigenere untuk melakukan enkripsi.

Pada gambar 4 bujur sangkar Vigenere, kolom paling kiri menyatakan huruf- huruf kunci, dan baris paling atas menyatakan *plainteks.* sedangkan karakter – karakter lainnya menunjukkan karakter cipherteks. Setiap baris di dalam bujur sangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher. pergeseran huruf mejadi cipherteks ditentukan oleh nilai decimal dari huruf kunci yang bersangkutan (a=0,b=1, …,y=24,z=25).

Vigenere Cipher telah berkali – kali diciptakan ulang dengan cukup bervariasi. Namun, metode aslinya digambarkan oleh Giovan Batista Belaso pada tahun 1553 seperti tertulis di dalam bukunya La Cifra del Sig. Giovan Batista Belaso. Meskipun demikian, Vigenere Cipher dipopulerkan oleh Blaise de Vigenere pada tahun 1586.



Gbr.4 Bujur Sangkar Vigenere

- Contoh penerapan Vigènere Cipher :
  - Plainteks : THIS PLAINTEXT
  - Kunci : sony sonysonys
  - Cipherteks : *LVVQ HZNGFHRVL*

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Dalam hal ini Kunci “sony” diulang sebanyak panjang plaintext-nya

- Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

c(‘T’) = (‘T’ + ‘s’) mod 26 = L
T = 20 dan s= 19 → (20+19)%26=13 → L
c(‘H’) = (‘H’ + ‘o’) mod 26 = V, dst

Oleh karena itu, berbagai varian Vigenere Ciper bermunculan. Hal tersebut terutama untuk menutupi kekurangan Vigenere Cipher yang terletak pada pengulangan kunci.

Varian Vigenere Cipher [7]

- *Full Vigenere Cipher*
  Setiap baris di dalam tabel tidak menyatakan pergeseran huruf, tetapi menyatakan permutasi huruf-huruf alphabet.
- *Auto-Key Vigenere Cipher*
  Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci disambung dengan plainteks tersebut sehingga panjang kunci menjadi sama dengan panjang plainteks.
  Misalnya :

  p (plainteks) : *KRIPTOGRAFI*
  k (kunci) : *LAMPIONKRIP*

- *Running-Key Vigenere Cipher*
  Kunci merupakan string panjang yang diambil dari teks bermakna. Misalnya :

p (plainteks) : *KRIPTOGRAFI*******
k (kunci) : *KEMANUSIAANYANG..*

- *One Time Pad*
  Panjang kunci sama dengan panjang plainteks. Masing – masing karakter kunci diperoleh secara acak.

Algoritma enkripsi dan dekripsi pada Vigenere Cipher memiliki beberapa karateristik [5], yaitu :

1. Hanya menampung 26 huruf alfabeth dalam bentuk huruf kecil, sedangkan tanda baca lain tidak dapat terbaca.
2. Inputan hanya menerima hasil dalam bentuk huruf kecil, apabila terdapat huruf capital harus dikonversian terlebih dahulu dalam bentuk huruf besar.
3. Panjang kunci yang diterima harus sama dengan panjang plaintext(Pi), sehingga membutuhkan memori yang sangat besar yang mengakibatkan proses jadi lama.

Enkripsi (penyandian) dengan sandi Vigenère juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$C_i \equiv (P_i + K_i) \mod 26$$

atau C = P + K kalau jumlah dibawah 26 & - 26 kalau hasil jumlah di atas 26 dan dekripsi,

$$P_i \equiv (C_i - K_i) \mod 26$$

atau P = C - K kalau hasilnya positif & + 26 kalau hasil pengurangan minus

Keterangan: C_i adalah huruf ke-i pada teks tersandi, P_i adalah huruf ke-i pada teks terang, K_i adalah huruf ke-i pada kata kunci, dan mod adalah *operasi modulus* (sisa pembagian).

IV. Implementasi dan Pembahasan

A. Kombinasi Kriptografi dan Steganorafi

Gbr. 5 Proses Kombinasi Kriptografi dan Steganografi

Pada gambar 5 dapat dilihat proses kombinasi kriptografi dan steganografi. Pesan teks (*plaintext*) yang akan disisipkan ke dalam citra digital terlebih dahulu dienkripsi dengan menggunakan metode *Vigenere Cipher*. Selanjutnya hasil enkripsi (*ciphertext*) disisipkan ke dalam sebuah citra digital melalui proses penyisipan dengan menggunakan LSB. Hasil penyisipan berupa citra hasil (*stego image*), dimana di dalam *stego image* ini telah terdapat pesan yang telah disisipkan sebelumnya. Ekstraksi pesan dilakukan dengan menggunakan metode yang sama saat proses penyisipan. Hasilnya adalah diperoleh pesan yang telah disisipkan sebelumnya (*ciphertext*). Selanjutnya pesan (*ciphertext*) didekripsi dengan menggunakan metode *Vigenere Cipher* sehingga menghasilkan pesan awal (*plaintext*).

Misalkan kalimat yang ingin sisipkan berupa teks (*plaintext*) “POTENSI“ dengan pergeseran nilai 4. Maka terlebih dahulu huruf-huruf tersebut diubah ke dalam bentuk kode ASCII, lalu kode ASCII tersebut ditambah dengan nilai pergeseran yang telah dimasukkan.
Karakter 0 = P dalam kode ASCII = 80
Karakter 0 = 80 + 4 = 84 => T
Karakter 1 = O dalam kode ASCII = 79
Karakter 1 = 79 + 4 = 83 => S
Karakter 2 = T dalam kode ASCII = 84
Karakter 2 = 84 + 4 = 88 => X
Karakter 3 = E dalam kode ASCII = 69
Karakter 3 = 69 + 4 = 73 => I
Karakter 4 = N dalam kode ASCII = 78
Karakter 4 = 78 + 4 = 82 => R
Karakter 5 = S dalam kode ASCII = 83
Karakter 5 = 83 + 4 = 87 => W
Karakter 6 = I dalam kode ASCII = 73
Karakter 6 = 73 + 4 = 77 => M

Pesan sebelum dienkripsi : POTENSI
Pesan sesudah dienkripsi : TSXIRWM

Lalu setelah pesan dienkripsi lalu pesan akan diubah ke dalam bentuk ASCII dengan nilai seperti terhihat pada tabel 3.

Tabel III.
Nilai ASCII dari Pesan

T	01010100	R	01010010
S	01010011	W	01010111
X	01011000	M	01001101
I	01001001		

Setelah diubah ke dalam bentuk ASCII lalu pesan akan disisipkan ke dalam citra dengan metode LSB dengan nilai biner piksel citra awal ditunjukkan pada tabel 4.

Tabel IV
Nilai Biner Piksel Awal

11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111
11111111	11111111	11111111	11111111	11111111	11111111	11111111	11111111

Setelah pesan disisipkan pada citra maka nilai biner piksel citra tersebut akan berubah seperti ditunjukkan pada tabel 5.

Tabel V.
Nilai Biner Piksel Citra Setelah Proses Penyisipan

11111110	11111111	11111110	11111111	11111110	11111111	11111110	11111110
11111110	11111111	11111110	11111111	11111110	11111110	11111111	11111111
11111110	11111111	11111110	11111111	11111111	11111110	11111110	11111110
11111110	11111111	11111110	11111110	11111111	11111110	11111110	11111111
11111110	11111111	11111110	11111111	11111110	11111110	11111111	11111110
11111110	11111111	11111110	11111111	11111110	11111111	11111111	11111111
11111110	11111111	11111110	11111110	11111111	11111111	11111110	11111111

Proses ekstraksi pesan dilakukan dengan cara mengambil nilai LSB dari setiap piksel yang ada. Hasil pengambilan nilai LSB dari setiap piksel ditunjukkan pada tabel 6.

TABEL VI.
NILAI BINER HASIL EKTRAKSI PESAN

01010100	01010011	01011000	01001001	01010010	01010111	01001101
T	S	X	I	R	W	M

Proses berikutnya pesan diubah dengan menggunakan pergeseran kembali tapi dengan menggunakan nilai pergeseran -4.

Karakter 0 = T dalam kode ASCII = 84
Karakter 0 = 84 - 4 = 80 => P
Karakter 1 = S dalam kode ASCII = 83
Karakter 1 = 83 - 4 = 79 => O
Karakter 2 = X dalam kode ASCII = 88
Karakter 2 = 88 - 4 = 84 => T
Karakter 3 = I dalam kode ASCII = 73
Karakter 3 = 73 - 4 = 69 => E
Karakter 4 = R dalam kode ASCII = 82
Karakter 4 = 82 - 4 = 78 => N
Karakter 5 = W dalam kode ASCII = 87
Karakter 5 = 87 - 4 = 83 => S
Karakter 6 = M dalam kode ASCII = 77
Karakter 6 = 77 - 4 = 73 => I

Pesan sebelum didekripsi : TSXIRWM
Pesan sesudah didekripsi : POTENSI

B. *LSB (Least Significant Bit)*

LSB *(Least Significant Bit)* merupakan salah satu metode dalam *steganography*. LSBdilakukan dengan mengambil bit – bit terakhir warna pada citra dan menggantinya dengan bit – bit data. Banyak cara yang dapat dilakukan untuk mengganti bit – bit warna pada citra, antara lain dengan melakukan operasi penambahan atau pengurangan nilai warna pada citra, atau juga dengan cara melakukan operasi AND dan OR antara bit – bit warna dengan bit – bit data. Tujuan utama dari LSB adalah memanipulasi nilai suatu titik warna *(pixel)* sehingga data dapat disembunyikan ke dalam titik warna tersebut namun perubahan yang terjadi berusaha diminimalisasi sehingga seakan – akan perubahannya tidak dapat dideteksi oleh mata manusia.

Pada penelitian ini, akan digunakan metode LSB (Least Significant Bit) yang merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu.Untuk menjelaskan teknik penyembunyian LSB yang dipakai ini kita menggunakan citra digital sebagai covertext. Setiap pixel yang ada di dalam file citra berukuran 1 sampai 3 byte. Pada susunan bit dalam setiap byte (1 byte = 8 bit) , ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB)
Mengganti Bit LSB menjadi Bit Data

LSB : Least Significant Bit
MSB : Most Significant Bit

Gbr. 6 Contoh LSB dan MSB

Dari contoh byte 11010010 pada gambar contoh LSB dan MSB diatas bit 1 pertama yang (di garis bawahi) adalah bit MSB dan bit 0 terakhir yang digaris bawahi adalah bit LSB. Bit yang cocok untuk diganti dengan bit pesan adalah bit LSB, karena modifikasi hanya mengubah nilai byte tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut di dalam gambar memberikan persepsi warna merah, maka perubahan satu bit LSB hanya mengubah persepsi merah tidak terlalu berarti karena mata manusia tidak dapat membedakan perubahan sekecil ini.
Sebagai ilustrsi misalkan cover-object adalah citra sekempulan citra berwarna merah seperti yang terlihat pada contoh di bawah ini:

00110011 10100010 11100010 01101111

Dan misalkan pesan rahasia (yang telah dikonversi ke system biner) embedded message adalah 0110. Setiap bit dari watermark menggantikan posisi LSB dari segmen pixel-pixel citra menjadi :

00110010 10100011 11100011 01101110

Dari hasil penanaman atau embedding kedalam sekumpulan pixel citra berwarna merah tadi diperoleh kembali sekumpulan pixel berwarna merah yang telah berubah sedikit pada posisi bit terendah atau LSB dari pixel tersebut. Demikianlah contoh sederhana bagaimana algoritma LSB bekerja untuk menggantikan nilai bit-bit terendah dari setiap pixel untuk disisipkan atau digantikan oleh bit baru yang mengandung pesan [3].

C. PROSES IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN ALGORITMA KRIPTOGRAFI (VIGENERE CIPHER)

Gbr. 7 sebelum penyisipan pesan

Gbr. 8 setelah penyisipan pesan

- Proses Penyisipan Pesan kedalam Gambar

Gbr. 9 penyisipan pesan kedalam gambar

Ujicoba Enkripsi Pesan menggunakan Vigenere Cipher dengan Software Matlab R2014b :

Program:

```
function StrOut = VigenereCrypt(str,keystr)
% StrOut = VigenereCrypt(str,keystr)
% Inputs: str = a string of lower case text (alphabet: a, b, ..., z)
%         keystr = a string of lower case text (alphabet: a, b, ..., z)
% Output: StrOut = a string of corresponding Upper-Case ciphertext (alphabet: A, B, ..., Z):
% resulting from encrypting str using the Vigenere cipher with key keystr
Vec = LCText2Int(keystr);
keylength = length(keystr);
for i=1:length(str)
   ishift = mod(i,keylength);
   if ishift == 0, ishift = keylength; end %corresponding to the last character of keystring
   StrOut(i) = ShiftCrypt(str(i),Vec(ishift));
end
```

Gbr. 10. Kode program untuk enkrip

Hasil Eksekusi Progam:

Gbr. 11. Hasil proses eksekusi program dalam (matlab)

Untuk mendapatkan pesan yang utuh kembali, yang harus dilakukan adalah masukan nilai hasil proses enkripsi sebelumnya : *VYJGFCTTULTMVOJMVSVC* kemudian masukkan kata kunci sebelumnya yaitu : *bl* , maka bisa didapatkan nilai hasil dari proses dekripsi :

ans = universitasbudiluhur

Kalau dilihat dari hasil eksekusi program :

'*universitasbudiluhur*' adalah pesan yang dikirimkan menggunakan spasi.
'*bl*' adalah kata kunci yang digunakan untuk membuka pesan yang kita enkripsikan.
ans = VYJGFCTTULTMVOJMVSVC
ans = Nilai Hasil dari proses enkripsi pesan dengan menggunakan algoritma Vigenere Cipher

- *Proses Dekripsi pesan*

Gbr. 12. Penyisipan pesan kedalam gambar

Program:

Gbr. 13. Kode program(matlab) dekrip pesan

Hasil Eksekusi Program **:**

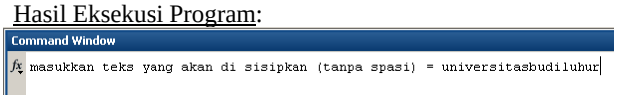
Gbr. 14. Hasil proses eksekusi program(matlab)

Untuk mendapatkan pesan yang utuh kembali, yang harus dilakukan adalah masukan nilai hasil proses enkripsi sebelumnya : *VYJGFCTTULTMVOJMVSVC* kemudian masukkan kata kunci sebelumnya yaitu : *bl* , maka bisa didapatkan nilai hasil dari proses dekripsi :

ans = universitasbudiluhur

- Menambahkan Program Enkrip/Dekrip kriptografi kedalam Program Steganografi

Hasil Eksekusi Program:



Gbr. 15. Eksekusi program masukkan pesan

Teks yang dimasukkan tanpa menggunakan spasi dikarenakan program *VigenerCrypt.m* di setting tidak menggunakan spasi, tujuannya agar mempermudah enkripsi teks.

Selanjutnya pada program akan di minta memasukan kunci kriptografi seperti dibawah ini

Gbr. 16 kode program (matlab) masukkan kata kunci

Tujuannya agar pesan yang disisipkan kedalam gambar tidak dapat terbaca infonya walau pada metode steganografinya berhasil di hack. Pada Program *VigenerCrypt.m* akan menjalankan program *LCText2Int.m* , dimana program tsb berfungsi untuk mengubah huruf menjadi nilai angka, dengantabel seperti dibawah ini :

TABEL VII.
TABEL HURUF

Sehingga hasil konversi huruf menjadi angka adalah :

ans = 20 13 8 21 4 17 18 8 19 0 18 1 20 3 8 11 20 7 20 17

Selanjutnya program akan menampilkan gambar sebelum disisipkan dan setelah disisipkan pesan, seperti dibawah ini:

Figure 1 : Gambar Asli Figure 2 : Gambar disisipi Pesan kriptografi

Gbr. 17 Hasil sebelum dan sesudah penyisipan

Sedangkan untuk membaca pesan yang di enkrip kedalam gambar , bisa dilakukan dengan menjalankan program *baca_pesan.m* menggunakan *matlab R2014b* seperti dibawah ini:

Program:

```
close all;clear;clc;
gambar=imread('result_picture.bmp');
[baris,kolom,rgb]=size(gambar);
counter=[1 1];r=1;lokasi=counter;
for i=1:8 %proses pengambilan 8 piksel (1huruf) dari gambar
    var(i)=gambar(counter(1),counter(2),r);%variabel var menyimpan piksel dr gambar
    counter(2)=counter(2)+1; %ini sama dgn counter yg tadi
    if counter(2)>kolom
        counter(2)=1;
        counter(1)=counter(1)+1;
    end
    lokasi(1,end+1)=counter(1);
    lokasi(1,end+1)=counter(2); % Lokasi menyimpan piksel2 mana saja yg diambil

end
% merubah piksel2 terambil menjadi binary
var1=dec2bin(var(1),8);var2=dec2bin(var(2),8);
var3=dec2bin(var(3),8);var4=dec2bin(var(4),8);
var5=dec2bin(var(5),8);var6=dec2bin(var(6),8);
var7=dec2bin(var(7),8);var8=dec2bin(var(8),8);
%Proses pengambilan bit terakhir menjadi informasi ttg panjang char pesan
%pjgpsn=zeros(1,8,'s');
pjgpsn(1)=var1(8); pjgpsn(2)=var2(8);
pjgpsn(3)=var3(8); pjgpsn(4)=var4(8);
pjgpsn(5)=var5(8); pjgpsn(6)=var6(8);
pjgpsn(7)=var7(8); pjgpsn(8)=var8(8);
pjgpsn=bin2dec(pjgpsn);
%Proses pengambilan teks dari gambar sesuai dgn pjg pesannya
for k=1:pjgpsn
    for i=1:8 %proses pengambilan 8 piksel (1huruf) dari gambar
        var(i)=gambar(counter(1),counter(2),r);%variabel var menyimpan piksel dr gambar
        counter(2)=counter(2)+1; %ini sama dgn counter yg tadi
        if counter(2)>kolom
            counter(2)=1;
            counter(1)=counter(1)+1;
        end
        lokasi(1,end+1)=counter(1);
        lokasi(1,end+1)=counter(2); % Lokasi menyimpan piksel2 mana saja yg diambil
    end
    % merubah piksel2 terambil menjadi binary
    var1=dec2bin(var(1),8);var2=dec2bin(var(2),8);
    var3=dec2bin(var(3),8);var4=dec2bin(var(4),8);
    var5=dec2bin(var(5),8);var6=dec2bin(var(6),8);
    var7=dec2bin(var(7),8);var8=dec2bin(var(8),8);
    %Proses pengambilan bit terakhir menjadi informasi ttg panjang char pesan
    %pjgpsn=zeros(1,8,'s');
    psn(k,1)=var1(8); psn(k,2)=var2(8);
    psn(k,3)=var3(8); psn(k,4)=var4(8);
    psn(k,5)=var5(8); psn(k,6)=var6(8);
    psn(k,7)=var7(8); psn(k,8)=var8(8);
end
psn=bin2dec(psn); psn=native2unicode(psn);
psn=psn';
vmsgcrypt=input('masukkan kata kunci (kriptografi) = ','s');
psn=VigenereDeCrypt(psn,vmsgcrypt);
disp(psn);
```

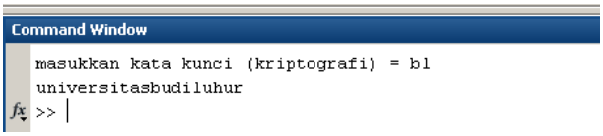
Gbr. 18 Kode Program (matlab) untuk dekripsi

Hasil Eksekusi Program adalah membaca pesan dari gambar yang disisipkan :

Va=0	**b=1**	**c=2**	**d=3**	**e=4**
Vf=5	**g=6**	**h=7**	**i=8**	**j=9**
J k=10	**l=11**	**m=12**	**n=13**	**o=14**
Gp=15	**q=16**	**r=17**	**s=18**	**t=19**
Fu=20	**v=21**	**w=22**	**x=23**	**y=24**
Cz=25				

TTULTMVOJWVSVC

Pesan diatas tidak bisa langsung terbaca karena masih dienkripsi menggunakan algoritma *Vigenere Cipher*, jadi program akan Menjalankan *VigenereDeCrypt.m* untuk proses dekripsi, bisa dilihat pada program diatas dari baris *53 s/d 56.* User diminta kembali untuk memasukkan kata kunci nya yaitu : *bl*, apabila kunci yang dimasukkan tidak sesuai dengan kunci pertama kali dimasukkan pada proses enkripsi maka pesan yang ditampilkan akan salah.



Gbr. 19. Inputan pesan enkripsi beserta kata kunci

A. PENUTUP

A. *Kesimpulan*

- Algoritma Kriptografi ada 2 macam yaitu Algoritma Kriptografi Klasik dan Algoritma Kriptografi Modern. Dalam Hal ini penulis menggunakan Algoritma Kriptografi Klasik dengan nama *Vigenere Cipher* untuk proses enkripsi pesan yang akan disisipkan kedalam gambar.
- Untuk proses penyisipan pesan kedalam gambar penulis menggunakan metode Steganografi Least Significant Bit atau dikenal dengan nama LSB sehingga pesan tidak terlihat pada gambar.
- Untuk ukuran file gambar sebelum dan sesudah disisipkan teks tidak terlalu berubah drastis karena menggunakan metode substitusi dan pengaruh pesan teks yang disisipkan tidak terlalu banyak.

B. *Saran*

- Pada uji coba menggunakan software matlab masih perlu adanya beberapa perbaikan pada program salah satunya dari segi tampilan agar tampil lebih visual.
- Masih ada keterbatasan pada input teks, dimana teks yang disisipkan harus huruf kecil dan tidak boleh ada spasi, kedepannya sebaiknya dihilangkan keterbatasan tersebut.

REFERENSI

[1] Prasetiyo, B. (2013). *Kombinasi Steganografi Bit Matching Dan Kriptografi Des Untuk Pengamanan Data.* Semarang: Universitas Diponegoro, Semarang.

[2] Ariyus, D. (2009). *Keamanan Multimedia.* Yogyakarta: Andi.

[3] Alatas, P. (2009). *Implementasi Teknik Steganografi Dengan Metode Lsb Pada Citra Digital* . Jakarta: Universitas Gunadarma.

[4] Cox, I., Miller, M., Bloom, J., & Fridrich, J. &. (2008). *Digital Watermarking and Steganography 2nd Ed.* Morgan Kaufmann., MA.

[5] Kipper, G. (n.d.). (2004). *Investigator's Guide to Steganography*, Florida: CRC Press LLC

[6] H. B. Kekre, A. A. (2008). *Increased Capacity of Information Hiding In Lsb's Method For Text And Image.* International Journal of Electrical, Computer, and Systems Engineering, Vol. 2, No. 4, p. 246-249.

[7] Abhirama, D. (-). *Keystream Vigenere Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator.* Bandung: Institut Teknologi Bandung.