ENKRIPSI CITRA BITMAP MELALUI SUBSTITUSI WARNA MENGGUNAKAN VIGENERE CIPHER

Arifin Luthfi P - 13508050
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

***Abstrak*— Citra merupakan representasi dari sebuah fakta yang terjadi di dunia pada saat tertentu. Citra juga dapat berisi sebuah pesan yang ditujukan untuk orang tertentu. Pada suatu saat, fail citra dapat menjadi aset berharga yang tidak boleh dilihat selain oleh orang yang bersangkutan. Untuk mencegah terjadinya hal-hal yang tidak diinginkan, seperti bocornya pesan rahasia yang terdapat dalam citra kepada publik, kita dapat melakukan enkripsi terhadap fail citra agar fail citra tersebut tidak dapat dilihat dan dimengerti pesan yang terkandung di dalamnya oleh orang yang tidak berhak.**

Enkripsi merupakan salah satu metode agar tampilan citra menjadi tidak dapat dimengerti jika dilihat secara langsung. Dengan kunci tertentu, tampilan citra dapat dikembalikan pada keadaan awal (didekripsi) sehingga orang yang dimaksud dapat membaca pesan yang terdapat dalam citra tersebut.

Fail citra dapat dienkripsi dengan cara merubah komponen-komponen warna yang ada dalam tiap pixelnya. Jika seluruh komponen warna diubah, maka citra bitmap tersebut sudah tidak dapat diketahui lagi makna sebenarnya. Enkripsi dapat dilakukan dengan metode enkripsi *Vigenere Cipher*. Metode ini dapat dilakukan terhadap citra bitmap karena kita dapat melakukan enkripsi terhadap susunan representasi warna yang terdapat dalam setiap pixel dalam fail bitmap tersebut.

***Kata Kunci*—Citra, Kriptografi, Vigenere Cipher, Bitmap, Manipulasi Warna.**

I. PENDAHULUAN

Kriptografi merupakan sebuah metode untuk menjaga kerahasiaan pesan dari pihak yang tidak berkepentingan. Pesan dirahasiakan dengan cara mengacak nilai-nilai yang terdapat didalamnya sehingga membuat pesan tersebut tidak memiliki arti lagi.

Citra dijital dapat diartikan sebagai sebuah pesan karena didalamnya terdapat sejumlah informasi. Kerahasiaan pesan yang terdapat dalam fail citra juga dapat dijaga dengan metode kriptografi.

Kriptografi pada citra dijital dilakukan dengan cara merubah informasi warna pada tiap pixel dari citra tersebut. Dengan berubahnya warna-warna di setiap pixel citra dijital, pesan yang terkandung dalam sebuah citra tidak dapat diketahui lagi.

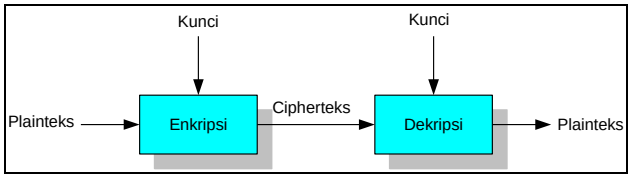
Banyak algoritma kriptografi yang bisa digunakan untuk memanipulasi warna yang terdapat dalam citra, salah satunya dengan algoritma kriptografi klasik seperti algoritma vigenere.

II. TERMINOLOGI

2.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Pesan dalam kriptografi dapat berupa tulisan, citra, video, dan sebagainya. Proses kriptografi dilakukan agar informasi yang terdapat didalam pesan tidak bocor kepada pihak yang tidak berkepentingan saat dilakukan pengiriman pesan.

Dalam kriptografi, pesan yang belum disandikan disebut plainteks, sedangkan pesan yang telah disandikan disebut cipherteks. Terdapat dua proses pada kriptografi yang berguna untuk menyandikan dan mengekstraksi pesan yang telah disandikan. Proses tersebut antara lain enkripsi dan dekripsi. Enkripsi adalah proses menyandikan plainteks menjadi cipherteks. Sedangkan dekripsi merupakan proses mengembalikan cipherteks menjadi plainteks semula, agar dapat diketahui informasi yang terkandung didalamnya.



Gambar 1: Flow diagram Kriptografi

Misalkan:
C = Chiperteks
P = Plainteks

Fungsi enkripsi E memetakan P ke C,
$E(P) = C$
Fungsi dekripsi D memetakan C ke P,
$D(C) = P$

Fungsi enkripsi dan dekripsi harus memenuhi sifat:
$D(E(P)) = P$

2.2 Citra Dijital

Dalam dunia dijital, sebuah citra merupakan array numerik yang merepresentasikan intensitas warna pada

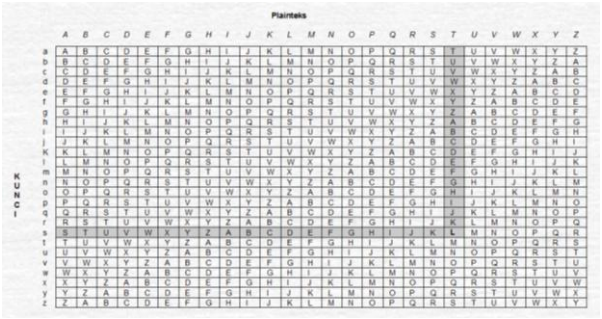
berbagai posisi titik (pixel). Dalam satu pixel pada citra dijital, biasanya terdapat informasi warna yang berukuran 8 – 32 bit. Informasi dalam satu pixel tersebut dapat dibagi menjadi beberapa komponen warna, misalkan citra dijital dengan intensitas warna 32 bit (4 byte), di dalamnya terdapat informasi warna merah (Red), hijau (Green), biru (Blue), dan transparansi (Alpha) yang masing-masing besarnya 1 byte.

Kombinasi dari empat komponen warna tersebut dapat menghasilkan warna baru untuk tampilan citra. Alpha sendiri merupakan nilai transparansi dari sebuah pixel. Jika bernilai penuh (255), maka dalam pixel tersebut warna ditampilkan tanpa adanya transparansi, sedangkan jika Alpha bernilai nol, pixel tersebut terlihat transparan.

Kumpulan pixel-pixel dengan warna tertentu dapat disusun menjadi sebuah citra yang memiliki makna, dimana terdapat informasi didalamnya.

2.3 Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Vigenere Cipher termasuk ke dalam cipher abjad-majemuk. Vigenere cipher menggunakan bujursangkar Vigenere untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher.



Gambar 2: Bujursangkat Vigenere

Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Bila panjang kunci adalah m, maka periodenya dikatakan m. Contoh :

```
Kunci awal = sony
Plainteks  : THIS PLAINTEXT
Kunci      : sony sonysonys
```

Dengan menggunakan bujursangkat Vigenere, hasil enkripsi seluruhnya adalah sebagai berikut :

```
Kunci awal = sony
Plainteks  : THIS PLAINTEXT
Kunci      : sony sonysonys
Cipherteks : LVVQ HZNGFHRVL
```

Huruf yang sama tidak selalu dienkripsi menjadi huruf cipheteks yang sama pula. Contohnya huruf plainteks **T** dapat dienkripsi menjadi **L** atau **H**, dan huruf cipherteks **V** dapat merepresentasikan huruf plainteks **H**, **I**, dan **X.** Hal ini merupakan karakteristik dari cipher abjad-majemuk, setiap huruf cipherteks dapat memiliki kemungkinan banyak huruf plainteks. Sedangkan pada Pada cipher substitusi sederhana, setiap huruf cipherteks selalu menggantikan huruf plainteks tertentu.

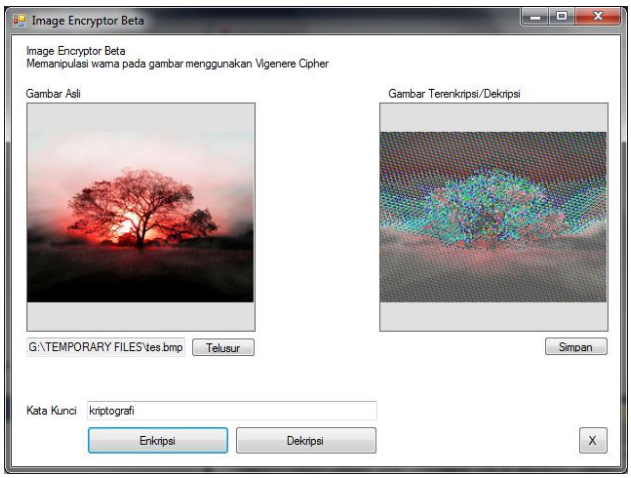
Vigenere Cipher dapat mencegah frekuensi huruf-huruf di dalam cipherteks yang mempunyai pola tertentu yang sama seperti pada cipher abjad-tunggal. Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search.*

III. LINGKUP MASALAH

Citra dijital sering kali merupakan sebuah arsip yang sangat rahasia. Citra dijital yang bersifat rahasia tidak boleh tersebar di publik sehingga publik tersebut mengetahui isi yang terdapat pada citra dijital tersebut. Untuk itu, perlu ada aplikasi yang berguna untuk melakukan enkripsi terhadap citra dijital agar ketika citra tersebut dikirimkan, publik tidak mengetahui isi yang ada didalamnya walaupun citra tersebut tersebar ke publik.

3.1 Program Enkripsi dengan Vigenere Cipher

Untuk melakukan enkripsi pada citra dijital, saya membuat sebuah program yang dapat memanipulasi kombinasi warna yang terdapat dalam sebuah citra. Tampilan antarmuka program tersebut kurang lebih sebagai berikut :



Gambar 3 : Tampilan Antarmuka Program

Pada gambar diatas, bagian kotak sebelah kiri merupakan gambar asli yang tidak dienkripsi, sedangkan sebelah kanan merupakan gambar yang telah dienkripsi dengan menggunakan program. Terlihat perbedaan antara gambar yang belum dienkripsi dan yang telah dienkripsi, gambar yang telah dienkripsi menjadi tidak jelas dan cukup sulit untuk dikenali. Enkripsi pada gambar diatas dilakukan dengan memanfaatkan algoritma kriptografi klasik Vigenere Cipher.

3.2 Metode Enkripsi Gambar

Enkripsi pada citra dilakukan dengan memanfaatkan algoritma Vigenere Cipher. Vigenere Cipher biasanya digunakan untuk mengenkripsi fail teks, namun kali ini dilakukan percobaan penggunaan Vigenere Cipher untuk mengenkripsi fail citra.

Proses enkripsi pertama-tama dilakukan dengan cara mengambil nilai warna dari sebuah citra. Nilai-nilai tersebut merupakan nilai dari komponen warna merah (Red), hijau (Green), biru (Blue), dan Alpha (tingkat transparansi). Nilai-nilai warna tersebut kemudian digabungkan menjadi sebuah string. String tersebutlah yang akan dienkripsi dengan menggunakan Vigenere Cipher.

Berikut contoh pengubahan nilai warna yang terdapat pada citra dijital. Misalkan :

Posisi Pixel	Nilai Warna (A-R-G-B)
0,0	255-100-150-150
0,1	255-100-140-140
0,2	255-100-130-130
0,3	200-200-150-175
0,4	200-125-125-125

Berdasarkan tabel diatas, kita dapat menyusun string dengan karakter-karakter bernilai asscii diatas. Hasilnya kurang lebih seperti dibawah ini :

Representasi String :

```
 dûû dîî déé╚╚û»╚}}}
```

Untuk melakukan enkripsi, dilakukan pengubahan informasi warna menjadi representasi dalam bentuk string untuk setiap pixel yang ada pada citra dijital. Dengan begitu, pada string yang didapat terdapat informasi seluruh warna yang terdapat dalam sebuah citra dijital.

Setelah dilakukan pengubahan menjadi string, kita dapat menggunakan metode Vigenere Cipher untuk melakukan pengacakan terhadap string tersebut. Jika string yang berisi informasi dari warna pada citra dijital diacak, maka warna-warna yang menyusun citra dijital tersebut akan berantakan dan citra dijital menjadi tidak memiliki makna yang sebenarnya.

Sebelum dilakukan proses enkripsi, kunci di set intensitasnya terlebih dahulu. Intensitas kunci merupakan sebuah nilai pengali dari kunci guna membuat kunci menjadi lebih kompleks dan perbedaan antara karakternya jauh. Intensitas diimplementasikan dalam source-code seperti berikut :

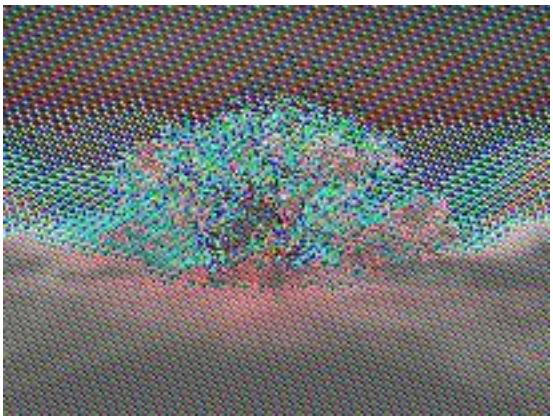
```
public byte[] generateKey(String key, byte[] content)
        {
            byte[] retVal = new byte[content.Length];
            for (int i = 0; i < content.Length; i++)
            {
                retVal[i] = (byte)((key[i % key.Length] *
                    this.intencity) % 256);
            }
            return retVal;
        }
```

Intensitas kunci tersebut diperlukan karena biasanya orang memasukkan kunci hanya berupa huruf alfabet. Perbedaan nilai byte pada huruf alfabet maksimal hanyalah 25 nilai (a-z). Pada pola warna, angka 25 bukanlah angka yang menyebabkan sebuah warna menjadi jauh berbeda. Untuk itu, perlu dikalikan dengan sebuah nilai intensitas agar pergeseran warna antara pixel satu dan pixel yang lain dapat terlihat jelas.

Enkripsi dilakukan dengan menggunakan Vigenere Table Extended, yang artinya tabel Vigenere berisi 256 karakter ascii, tidak seperti tabel standar yang hanya berisi 26 karakter alfabet. Setelah dilakukan enkripsi dengan Vigenere Cipher, string tersebut akan berubah nilainya. Nilai yang terdapat pada string yang telah dienkripsi kembali dimasukkan ke dalam citra sesuai dengan proses pengambilan informasi warna.

Setelah dilakukan pengisian informasi warna pada citra dengan representasi string yang telah dienkripsi, citra akan berubah karena warna-warna dalam setiap pixel citra dijital telah berubah. Berikut merupakan contoh citra sebelum dan setelah dilakukan proses enkripsi.

Gambar 4 : Citra Sebelum Proses Enkripsi



Gambar 5 : Citra Setelah Proses Enkripsi

Dari gmabar diatas, terlihat bahwa gambar 5 terlihat buram, ini karena informasi warna yang terdapat dalam citra sudah diacak. Namun begitu, gambar masih terlihat polanya, ini kemungkinan karena proses enkripsi dengan Vigenere Cipher melakukan enkripsi dengan pengulangan

dengan interval tertentu (sesuai panjang kunci).

3.3 Metode Dekripsi Gambar

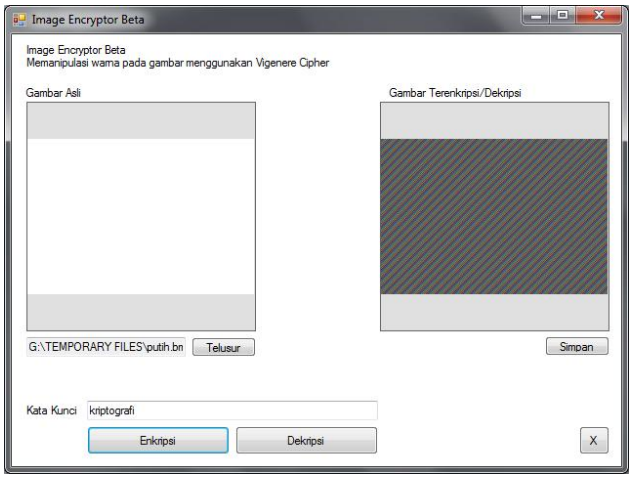
Proses dekripsi terhadap gambar yang telah dienkripsi hampir sama dengan proses enkripsi. Pertama-tama informasi warna pada gambar diubah menjadi representasi string. String yang ada kemudian didekripsi dengan fungsi yang relevan dengan fungsi enkripsi. Setelah itu, string hasil dekripsi kemudian kembali dikodekan menjadi informasi warna pixel yang ada pada citra dan dimasukkan kembali.

Hasil dekripsi akan sama persis dengan citra dijital sebelum di enkripsi. Ini karena representasi warna dalam string sebelum proses enkripsi dan setelah proses dekripsi akan sama.

IV. ANALISIS HASIL

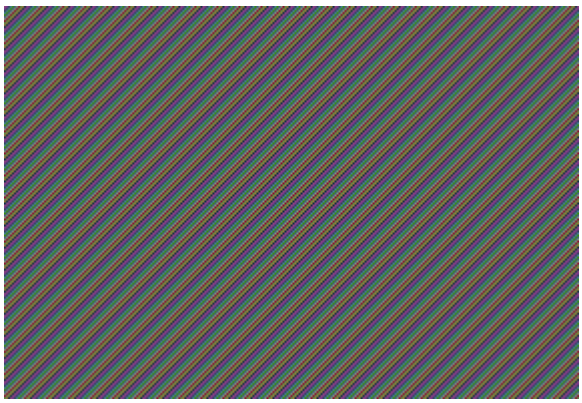
Bisa dilihat pada perbedaan citra dijital sebelum dan setelah dilakukan enkripsi dengan metode Vigenere Cipher. Namun dapat dilihat juga, citra hasil enkripsi dengan kunci "kriptografi" masih memiliki garis besar pola yang sama dengan citra sebelum proses enkripsi. Ini mungkin dikarenakan pengulangan yang pada vigenere cipher, maksudnya ada warna yang sama yang dapat dienkripsi menjadi warna yang sama lagi untuk pixel-pixel tertentu pada batas pengulangan. Ini menyebabkan masih terlihatnya pola gambar secara garis besar.

Pola pengulangan yang jelas dapat dilihat pada contoh kasus dibawah ini. Akan dicoba mengenkripsi citra dijital yang warnanya homogen (putih).



Gambar 6 : Enkripsi Citra dengan Warna Homogen

Untuk lebih jelasnya, hasil enkripsi citra dijital dengan warna homogen dan kata kunci "kriptografi" dapat dilihat pada gambar dibawah.



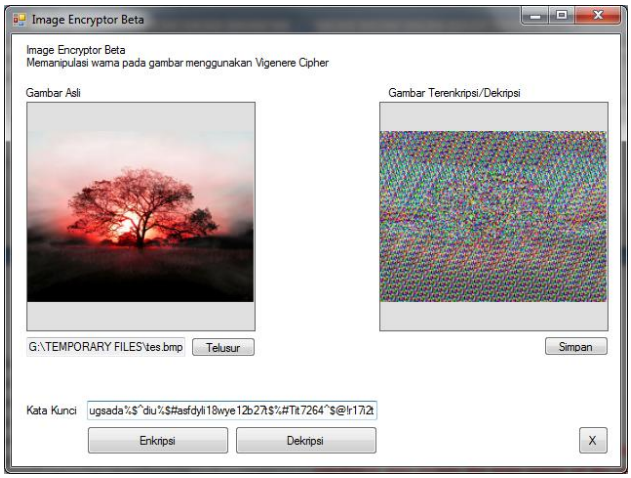
Gambar 7 : Hasil Enkripsi Citra dengan Warna Homogen

Terlihat dengan jelas terdapat garis-garis diagonal yang terbentuk pada citra diatas. Komposisi warna tersebut merupakan hasil enkripsi yang berulang sesuai panjang kunci yang dipilih.

Selanjutnya kita mencoba untuk melakukan enkripsi dengan kata kunci yang cukup panjang. Kita akan melakukan enkripsi citra yang sama seperti pada gambar 4 diatas. Hasil enkripsi citra dapat dilihat melalui gambar berikut :

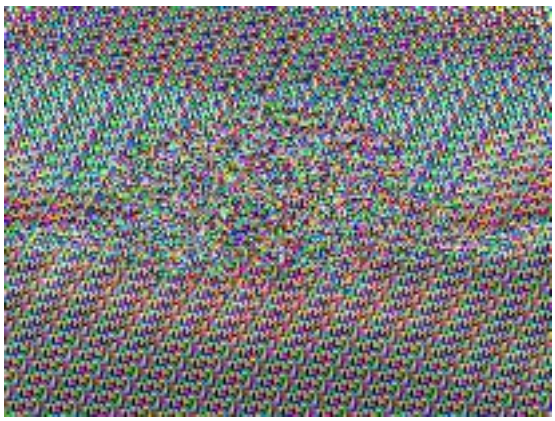
Kunci :

```
a23)(*sd!@$w23sa^%2gugsada%$^diu%$#as
fdyli18wye12b27t$%#Tit7264^$@!r17i2t
```



Gambar 8: Enkripsi dengan Kunci Panjang

Dengan kunci yang cukup panjang, dapat dilihat bahwa garis besar pola yang terdapat pada gambar hasil enkripsi relatif tidak terlihat. Untuk lebih jelasnya lihat gambar dibawah :



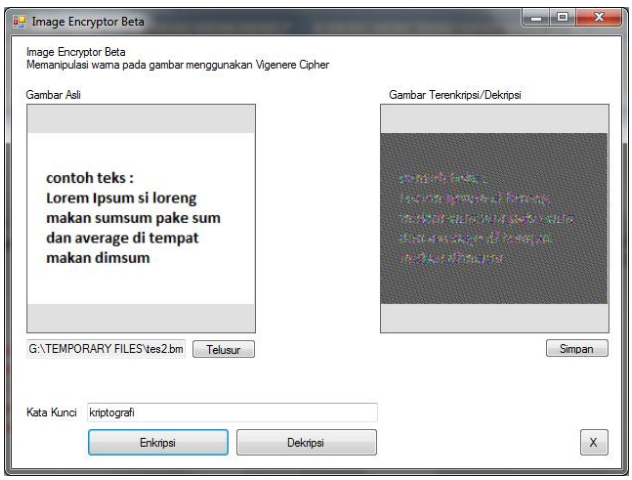
Gambar 9 : Citra yang sudah Dienkripsi dengan Kunci Panjang

Dengan kunci yang relatif panjang, hasil enkripsi dari gambar menjadi sulit untuk diterka gambar aslinya seperti apa. Komposisi warna pada citra hasil enkripsi menjadi teracak secara lebih beragam. Ini dikarenakan pengulangan yang terjadi jaraknya cukup jauh, sehingga sulit dilihat secara kasat mata oleh manusia.

Namun begitu, kata kunci yang panjang dan kompleks akan sangat sulit untuk diingat oleh manusia, hal ini nampak sia-sia karena jika kita memakai kata kunci yang panjang dan kompleks, kita harus meletakkannya pada suatu fail khusus untuk kunci tersebut. Jika fail yang berisi kunci tersebut bocor pada publik, maka enkripsi citra ini akan sia-sia karena dapat didekripsi dengan mudah.

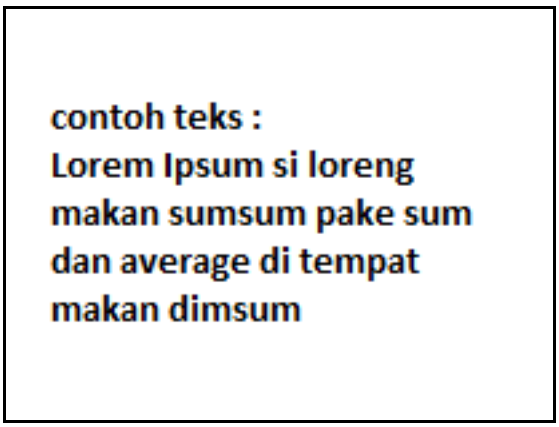
Kata kunci yang pendek cukup efektif untuk melakukan enkripsi citra yang berisikan tulisan yang tidak terlalu besar. Tulisan akan sulit dibaca walaupun kata kunci yang digunakan pendek. Ini dikarenakan untuk citra yang berisi pesan tulisan, kita tidak mendapat informasi berdasarkan gambar/pola yang kita lihat melainkan tulisan yang terdapat didalamnya.

Contoh dari enkripsi citra dijital yang berisikan tulisan adalah sebagai berikut (kunci = “kriptografi”) :

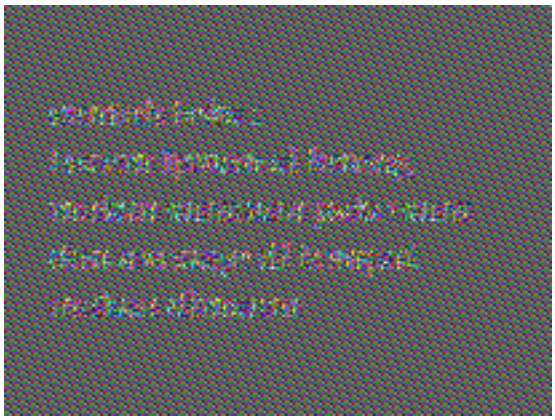


Gambar 10 : Enkripsi Citra yang Berisi Tulisan

Lebih jelasnya, dapat dilihat citra sebelum proses enkripsi dan setelah proses enkripsi dilakukan :



Gambar 11 : Citra Tulisan Asli



Gambar 12 : Citra Tulisan Hasil Enkripsi

Terlihat bahwa pada citra hasil enkripsi, tulisan yang terdapat di dalamnya tidak dapat dilihat dan dimengerti maknanya. Tidak seperti gambar yang dapat diterka maknanya dengan pola yang terlihat.

Walaupun dengan kunci yang pendek dan mudah diingat, tulisan yang terdapat dalam citra tidak dapat diketahui lagi maknanya. Oleh karena itu, enkripsi citra dengan metode Vigenere Cipher masih dapat diterima untuk menyembunyikan pesan yang terdapat pada citra yang berisikan sebuah tulisan/teks.

V. SIMPULAN

Vigenere Cipher merupakan metode enkripsi klasik yang dapat digunakan untuk melakukan enkripsi pada teks (string). Enkripsi dengan menggunakan metode Vigenere Cipher pada citra dijital dimungkinkan karena kita dapat mengubah informasi warna yang ada pada setiap pixel citra dijital menjadi representasi dalam bentuk string, string inilah yang kemudian akan kita lakukan enkripsi maupun dekripsi untuk merubah informasi warna yang ada pada citra dijital.

Enkripsi pada citra dijital dengan metode Vigenere Cipher masih dirasa kurang cocok. Ini dikarenakan proses enkripsi dengan menggunakan metode Vigenere Cipher pada citra dijital menghasilkan pola perulangan yang

membuat warna pada citra tidak teracak secara sempurna. Citra yang telah dienkripsi masih dapat terlihat polanya secara garis besar. Untuk citra biasa, makna dari sebuah citra biasanya masih dapat dilihat dari polanya. Ini membuat enkripsi dengan Vigenere Cipher menjadi kurang aman.

Enkripsi citra dengan menggunakan Vigenere Cipher masih dapat dilakukan dengan kunci yang relatif pendek terhadap citra yang mengandung tulisan/teks yang ingin dienkripsi. Ini dikarenakan setelah citra dienkripsi pola tulisan tersebut tidak jelas terlihat dan sulit untuk diketahui maknanya.

REFERENSI

[1] Munir, Rinaldi. 2011. Bahan Kuliah IF3054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] http://en.wikipedia.org/wiki/BMP_file_format, tanggal akses 15 Maret 2011

[3] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher, tanggal akses 15 Maret 2011

[4] http://msdn.microsoft.com/en-us/library/a343dky2(v=vs.90).aspx, tanggal akses 15 Maret 2011

PERNYATAAN

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

Bandung, 23 Maret 2011

Arifin Luthfi P
13508050