Penerapan dari Pengembangan Algoritma Vigenere dalam Enkripsi Image

Lea Angelina (13506117)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*xcoldblizzard@itb.ac.id*

Abstraksi

Algoritma kriptografi klasik vigenere adalah sebuah algoritma kriptografi klasik yang terkenal. Cara kerjanya sangat sederhana, dan pada umumnya algoritma ini digunakan untuk mengenkripsi pesan teks. Di sini, akan dicoba penerapan suatu algoritma baru yang merupakan semacam pengembangan/modifikasi dari algoritma vigenere, yang digunakan untuk mengenkripsi file image. Algoritma ini berbentuk stream cipher. Di sini, inspirasi utamanya adalah algoritma vigenere, akan tetapi dilakukan beberapa modifikasi, semisal: Pada algoritma vigerene biasa, enkripsi dilakukan pada teks per karakter, tetapi pada algoritma ini, enkripsi dilakukan pada file image dan operasinya per byte dan menggunakan operasi logika XOR.

Kata kunci: vigenere, enkripsi image, *stream cipher*

I. PENDAHULUAN

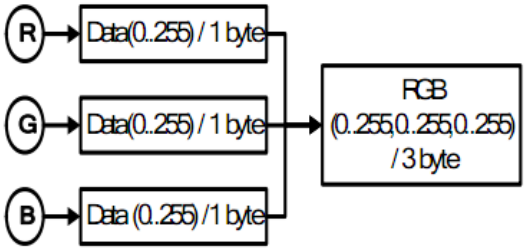
Perkembangan ilmu pengetahuan telah mendorong kemajuan di segala bidang kehidupan manusia. Salah satunya adalah bidang komputasi yang menggunakan komputer sebagai alat bantunya. Belakangan ini komputer telah berkembang dengan pesatnya dan dipergunakan secara luas dalam setiap aspek kehidupan untuk mempermudah dan mempercepat pekerjaan manusia yang tadinya dikerjakan secara manual. Walaupun sangat berguna, tetapi kemampuannya yang luas bisa saja dimanfaatkan oleh sebagian oknum untuk kepentingan-kepentingan jahat. Salah satunya adalah pencurian data. Pencurian dapat dilakukan dengan menyadap informasi yang ada. Contoh lainnya adalah pemodifikasian data yang dilakukan dengan mengganti informasi penting dari data yang telah dicuri demi kepentingan sang pencuri. Hal ini tentunya akan terasa kerugiannya bila informasi tersebut bersifat rahasia. Maka itu, diciptakanlah sebuah bidang yang berkonsentrasi dalam pengamanan data, yang bernama kriptografi.

II. IMAGE

Image adalah kumpulan pixel dalam bidang 2 dimensi yang mempunyai lebar dan tinggi tertentu. Berdasarkan jumlah warna, image dapat dibedakan menjadi tujuh jenis.

Nama	Jumlah Bit	Jumlah Warna
B/W	**1**	**2**
Windows Display	**4**	**16**
Grey Scale	**8**	**256**
256 Color	**8**	**256**
High Color	**16**	**65.535**
True Color	**24**	**16.777.216**
True Color	**32**	**4.294.967.296**

Warna pada image digital mempunyai beberapa representasi. Salah satunya adalah kombinasi dari tiga buah warna, yaitu merah, hijau, dan biru (Red, Green, and Blue/RGB), atau disebut juga dengan warna primer. Kombinasi dari nilai-nilai tertentu dari tiga buah warna itulah yang menciptakan suatu warna pada image. Pada image bitmap 24-bit yang digunakan pada ujicoba, nilai RGB memiliki rentang antara 0 sampai dengan 255 (8-bit/1 byte) per warna. Dengan demikian, jumlah variasi warna image tersebut adalah 16.777.216 warna.
Gambar ini menunjukkan sebuah warna dapat dihasilkan dari kombinasi tiga warna primer



III. ALGORITMA VIGENERE

Vigenere cipher adalah salah satu bentuk sederhana dari substitusi polyalphabetic. Vigenère cipher telah diciptakan beberapa kali, dengan penemu pertamanya adalah Giovan Battista Bellaso dalam bukunya La cifra del. Sig. Giovan Battista Bellaso yang diterbitkan pada tahun 1553. Vigenere cipher adalah metode untuk mengenkripsi teks alfabet menggunakan seri Caesar cipher yang berbeda-beda, berdasarkan huruf-huruf pada kunci. Jika semua huruf pada kunci telah selesai digunakan, maka siklus akan berulang kembali menggunakan kunci yang sama.
Ilustrasi sederhana vigenere cipher:

Plaintext:
HELLOMYNAMEISLEAANGELINAANDIAMTWENTYTWOYEARSOLD

Key:
VIGENEREVIGENEREVIGENEREVIGENEREVIGENEREVIGENER

Ciphertext:
DNSQCEDWHRSAXULFFFLAUPSOSSZPORYSNUYMLBKFJOWKKUK

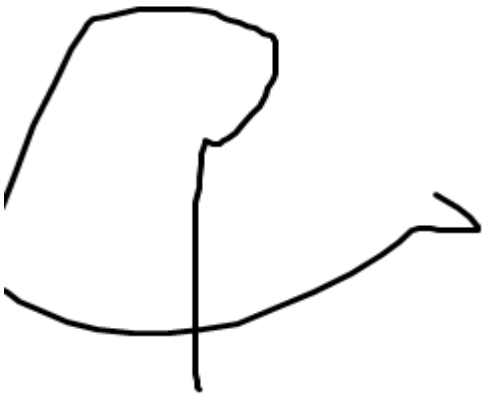
Cipher ini hanya bergantung pada metodologi confusion untuk membuat cipher text. Pola berulang pada plain text tidak melalui difusi, melainkan hanya dikamuflase oleh seri dari pergeseran Caesar cipher.
Vigenere cipher dianggap *unbreakable* selama hampir 300 tahun. Tetapi akhirnya metode untuk memecahkannya ditemukan oleh Kasiski dan Kerckhoff. Kedua metode berdasar pada fakta bahwa kuncinya berulang dan pada umumnya bahasa yang digunakan sehari-hari bersifat repetitif. Jika pesan jauh lebih panjang dari kunci, pada akhirnya kunci akan mengenkripsi satu kumpulan huruf yang sama yang sebelumnya telah digunakan dan dienkripsi oleh kunci yang sama. Hal ini akan menciptakan suatu pola yang berisi kumpulan huruf yang berulang. Dengan mencari frekuensi antara kumpulan huruf yang berulang dan memfaktorkannya, bisa ditemukan panjang kunci. Jika panjang kunci sudah diketahui, kunci akan dengan mudah diketahui dengan menggunakan analisis frekuensi pada setiap kumpulan Caesar cipher. Makin panjang kunci, akan makin sulit dan makin panjang proses penemuan kunci. Faktanya, jika kuncinya paling tidak sama panjang dengan panjang plaintext, cipher text kebal dari serangan tersebut. Cipher di mana panjang kunci sama dengan panjang pesan disebut one time pad.
Dengan kemajuan perkembangan teknologi dan makin kompleksnya komputer, vigenere cipher makin mudah untuk dipecahkan. Kebanyakan cipher text dapat dipecahkan dalam waktu beberapa detik bahkan dengan kunci yang panjang. Cipher ini sekarang dianggap sangat mudah untuk dipecahkan dan tidak memiliki keamanan yang berarti pada standar zaman sekarang. Walaupun demikian, vigenere digunakan di algoritma enkripsi yang lebih kuat seperti misalnya Advance Encryption Standard (AES). Karena ketika operasi eksklusif OR (XOR) digunakan dengan kunci biner dan pesan, itu adalah salah satu bentuk vigenere cipher.
Pada umumnya algoritma klasik semacam vigenere hanya bekerja pada file teks, tidak pada file jenis lainnya, karena zaman dahulu belum ada file digital, tetapi proses dekripsi enkripsi hanya dilakukan di atas kertas. Metode yang digunakan pada pemrosesan dengan menggunakan metode vigenere pada komputer antara lain tabel konversi dan operasi nilai ASCII, tetapi tidak bisa diterapkan pada image, diperlukan suatu adaptasi agar algoritma semacam itu bisa bekerja pada image. Maka itu, akan dilakukan modifikasi untuk membuat algoritma vigenere bisa mengenkripsi image. Algoritma modifikasi dari vigenere ini sangat sederhana, walaupun tidak diketahui seberapa efektivitasnya.

IV. DESKRIPSI ALGORITMA BARU

Algoritma ini memiliki kelebihan dibanding algoritma vigenere biasa, yaitu mampu mengenkripsi image (Algoritma vigenere biasa hanya dapat mengenkripsi teks).
Enkripsi dan dekripsi menggunakan kunci yang sama. Jika tidak, proses dekripsi tidak dapat menghasilkan image yang sama seperti image aslinya.

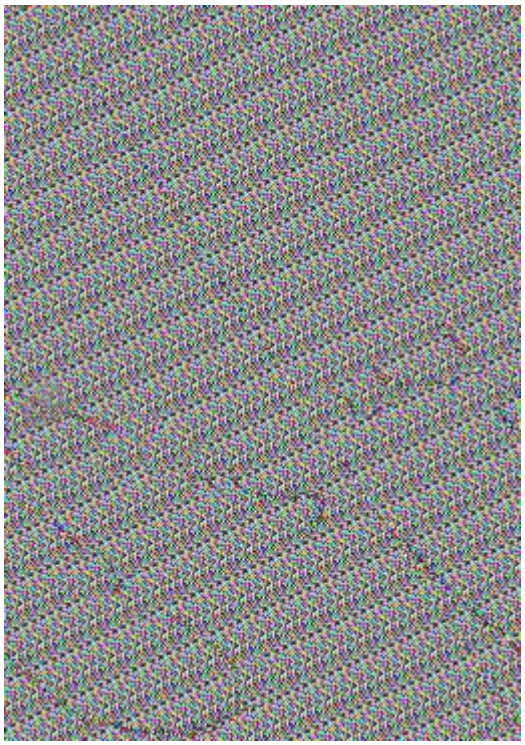
V. APLIKASI ALGORITMA

Image Awal:



Gambar 1. Gambar asli untuk ujicoba menggunakan gambar sederhana

Hasil Enkripsi dengan menggunakan string “halohaloimageiniakandiconvert” sebagai key adalah



Gambar 2. Hasil enkripsi gambar sederhana

Dilakukan sebuah pengembangan yaitu dari sisi key generation. Kelemahan penggunaan key biasa adalah hasil enkripsinya yang kurang kompleks karena karakter yang umum diketikkan oleh user awam adalah terbatas, yaitu hanya pada abjad a-z, baik huruf kecil maupun huruf besar, dan angka 0-9 sehingga nilai kunci kurang bervariasi. Pada algoritma yang sederhana seperti vigenere dan algoritma-algoritma lain yang menyerupainya, kerumitan kunci sangat mempengaruhi hasil enkripsi karena operasi yang digunakan pada algoritmanya juga sangat sederhana sehingga tidak memodifikasi gambar dengan sangat signifikan. Untuk mengatasi kelemahan tersebut, dilakukan pembangkitan kunci.

```
 private string keygen(string keyin)
 {
     char[] arrkey = keyin.ToCharArray();
     int total=0;
     StringBuilder sout = new
StringBuilder();
     string output = "";
     int size;
     for (int i = 0; i < arrkey.Length; i++)
     {
         total = total + (arrkey[i] *
arrkey[i]);
     }
     total = (int)Math.Sqrt(total);
     Random r = new Random(total);
     size = (int)Math.Sqrt(inputimage.Height
* inputimage.Width);
     for (int j = 0; j < size; j++)
     {
         sout.Append((char)r.Next(256));
     }
    output=sout.ToString();
    return output;
}
```

Snippet 1. Pembangkitan Kunci

Cara kerja pembangkit kunci tersebut adalah:

1. Ketika user mengetikkan key sebagai masukan, nilai ASCII dari karakter yang diketikkan akan diambil dan dikonversi ke dalam nilai integer.
2. Dicari akar dari nilai total kuadrat dari tiap-tiap nilai karakter
3. Nilai akar tersebut digunakan sebagai seed untuk pembangkitan sebuah nilai pseudorandom.
4. Ditetapkan jumlah kunci yang akan dibangkitkan adalah sejumlah kuadrat dari hasil kali nilai tinggi gambar dan lebar gambar, karena asumsinya, makin besar gambar, makin diperlukan kunci yang panjang, kunci pendek pada gambar yang berukuran besar akan menciptakan pola berulang sehingga lebih mudah diterka.
5. Dibangkitkan nilai ASCII random sesuai panjang kunci tersebut.

Sebagai contoh, pada gambar 2 tadi, string “halohaloimageiniakandiconvert” menghasilkan kunci

```
üÅ~__ÎÙæ__}±Ê~Da_Æ_¢kq'Ïw□#>¶T?T_@Sl\'ÉRÌ«©çàì_
¼l?*%h?□®??ª?0Ø(??+Ø_äýO?Æ}ç??Ä?IÐ_/²ÈÎ-?.^·? Ñ
¾Jb3äg?__?Ä_Æô_å_æ:ÃùäibWGÎ«?_%¬)K0??á0ç_? _®ç§
&y?´f_ÅfùÐÚ_W^n□}?s□¨×Ty_ÛãJÉ^[p?§2øN¾□cå7ÀÄÒÙ?
§_"d:JþO$%¯]3â_0r~?·¶;?.àÖ9Ã??µ3/R;3¦ù!& XÒ?`i□
É_NE2!Òl□ó?c_;°□o|-à¦è?x]y_^-·□?l·ù?Eo
```

Nilai kunci di atas tergolong aman dan variatif untuk mengkonversi gambar karena menghasilkan variasi warna pixel yang luas. Sedangkan jika menggunakan kunci yang umum digunakan user tanpa proses pembangkitan kunci, range nilai yang dihasilkan kecil sehingga variasi warna pixel yang dihasilkan terbatas. Pada hasil enkripsi, jika variasi warna yang dihasilkan terbatas, pola gambar akan lebih mudah terdeteksi oleh mata. Terutama jika gambarnya sederhana, dengan garis-garis yang tegas dan jelas. Bandingkan hasil enkripsi pada gambar 2 dengan gambar 3.

Gambar 3. Enkripsi gambar tanpa pembangkitan kunci acak

Pada enkripsi tanpa pembangkitan kunci, terlihat jelas garis-garisnya, dan dapat disimpulkan bahwa gambar itu hanya terdistorsi. Variasi warna yang dihasilkan terbatas karena rentang nilai ASCII pada alfabet huruf kecil hanya 26 sehingga hanya dihasilkan warna abu-abu. Meskipun pola yang serupa terlihat di bagian bawah gambar, tetapi pada hasil enkripsi dengan pembangkitan kunci secara acak, pola itu lebih tersamar.

Tahap enkripsi sangat sederhana, yaitu:

1. Konversi gambar ke byte
2. Konversi kunci yang sudah melalui tahap pembangkitan ke byte
3. Lakukan enkripsi seperti pada snippet 2.
4. Konversi byte ke gambar seperti pada snippet 3.

```
private byte[] convertAll(byte[] im, byte[]
txtkey)
{
     int imglength = im.Length;
     byte[] conversion = new byte[imglength];
     byte[] txtkey2 = new byte[imglength];
     if (txtkey.Length < imglength)
     {
         int b = 0;
         for (int a = 0; a < imglength; a++)
         {
             if (b < txtkey.Length)
             {
                 txtkey2[a] = txtkey[b];
                 b++;
             }
             else
             {
                 b = 0;
                 txtkey2[a] = txtkey[b];
                 b++;
             }
         }
     }
     for (int i = 0; i < imglength; i++)
     {
         conversion[i] = (byte)(txtkey2[i] ^
im[i]);
     }
     return conversion;
 }
```

Snippet 2. Konversi gambar

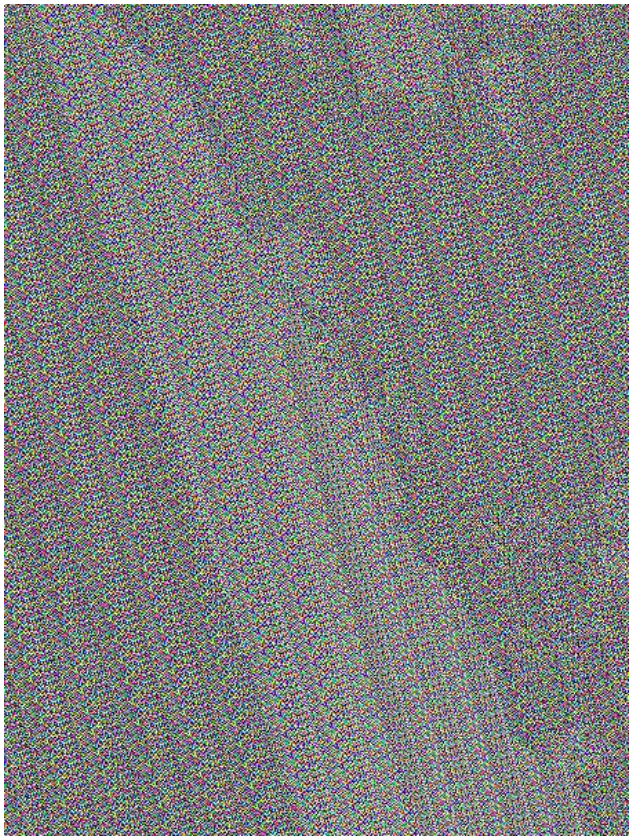
Penjelasan proses di atas adalah sebagai berikut:

1. Dibuat sebuah array txtkey2 yang berukuran sama dengan ukuran image.
2. Array txtkey2 itu diisi dengan kunci, dan jika karakter kunci sudah habis, maka kunci akan diulang dari awal sampai semua field pada array txtkey2 terisi penuh.
3. Byte pada array pixel image di-XOR-kan dengan byte pada array txt2.

Berikutnya, algoritma akan dicoba diaplikasikan pada gambar yang lebih kompleks

Gambar 4. Gambar asli untuk ujicoba dengan gambar kompleks

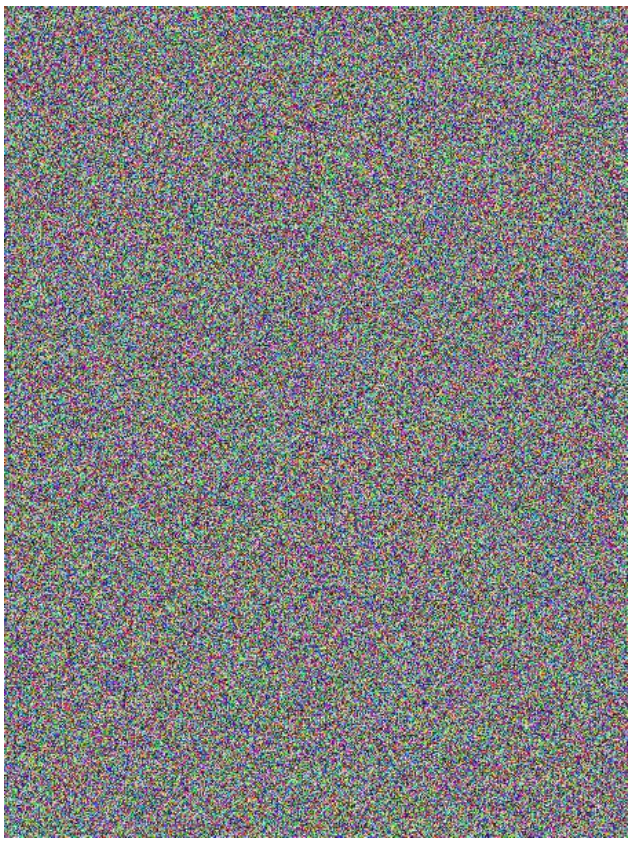
Hasil enkripsinya adalah sebagai berikut:



Gambar 5. Gambar hasil enkripsi menggunakan gambar kompleks

Pada hasil ujicoba berikutnya, dicoba menggunakan gambar yang lebih kompleks, yang terdiri dari variasi warna yang lebih banyak daripada gambar sederhana yang dipakai sebelumnya, dan hasilnya adalah seperti di atas. Gambar cukup tersamarkan walaupun siluet gambar yang terdistorsi dan terbalik masih sedikit terlihat, tetapi detail image sudah tidak terlihat sama sekali.

Jika enkripsi gambar dilakukan hanya satu kali, hasilnya memang kurang baik karena bentuk gambar masih bisa diterka, terlihat dari area gambar yang lebih gelap dibandingkan dengan area gambar yang lebih terang. Akan tetapi jika konversi gambar dilakukan dua kali dengan kunci yang berbeda, gambar hasil enkripsi yang dihasilkan akan baik karena bentuk gambar asli tidak terdeteksi sama sekali, disebabkan oleh banyaknya noise yang ada.



Gambar 6. Hasil enkripsi kedua menggunakan gambar kompleks

VII. KESIMPULAN

Seperti yang telah disebutkan sebelumnya, One time pad (OTP) kemungkinan adalah satu-satunya algoritma yang aman pada saat ini. Kekurangannya adalah kunci harus random dan panjang kunci harus sama dengan panjang pesan. Jika kunci dengan panjang m bisa dikirim secara rahasia, artinya pesan dengan panjang m harusnya juga bisa dikirim secara rahasia. Jika begitu, one time pad tidak ada gunanya. Sedangkan pada algoritma ini, pengiriman kunci menjadi lebih praktis karena menggunakan kunci biasa, yang akan dikonversi menjadi kunci yang lebih panjang dan lebih random pada saat proses enkripsi berlangsung. Mengapa tidak dikonversi menjadi kunci yang sama panjangnya dengan file pesan, karena faktor kecepatan menjadi pertimbangan. Apabila ukuran pesan besar, maka proses enkripsi akan menjadi sangat lambat. Diasumsikan panjang kunci yang dibangkitkan cukup panjang untuk tidak menciptakan pola yang berulang. Jadi walaupun vigenere cipher bukan merupakan algoritma yang aman, dengan adanya pengembangan ini, keamanan dari vigenere cipher bisa ditingkatkan.

VIII. DAFTAR PUSTAKA

[1] [1] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[2] [2] M.A.B. Younes, A. Jantan. “Image Encryption Using Block-Based Transformation Algorithm”. IJCSNS, 2008.
[3] [3] Schneier, Bruce.Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. 1995.
[4] [4] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004, p.38. http://www.enformatika.org/.

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, 29 April 2010

ttd

Lea Angelina
13506117