Modifikasi Watermark Menggunakan Kriptografi Klasik Pada Media Broadcasting

Dimas Aditiya Nurahman-13508093
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18093@students.if.itb.ac.id

Abstraksi— Dewasa ini pertukaran informasi yang ada sudah sebagian besar menggunakan file digital. File digital tersebut dapat disebarluaskan melalui media *broadcast* dalam bentuk gambar, audio atau video. Sebagaimana kita ketahui *content* dari sistem *broadcasting* dapat mudah disebarluaskan tanpa izin dari hak cipta pemilik file tersebut. Salah satu cara yang dapat digunakan untuk mengangani masalah ini adalah dengan menggunakan metode watermarking. Watermarking adalah suatu cara penyembunyian atau penanaman informasi tertentu (dalam bentuk digital maupun informasi teks) ke dalam suatu data digital lainnya. Sebagai tanda untuk membuktikan bahwa media yang digunakan saat *bradcasting*, maka *copyright* dari pemilik hak cipta media tersebut disipkan ke dalam bentuk *watermark* atau dapat kita kenal tanda air.. Untuk meningkatkan keamanan, pada makalah ini akan digunakan proses enkripsi dan dekripsi pada *watermark* yang disisipkan pada media yang ingin "diselamatkan". Watermarking yang akan dibahas di sini adalah watermarking yang sifatnya *invisible* karena data berupa image atau file teks lainnya yang disisipkan di sini akan di enkripsi terlebih dahulu menggunakan algoritma kriptografi. Pada makalah ini media *broadcasting* yang akan dibahas pada pengujian adalah berupa enkripsi dekripsi *watermark* yang nantinya akan disisipkan pada suatu frame.

Kata Kunci— *watermark, copyright, kriptografi, klasik, broadcast*

I. PENDAHULUAN

Media *broadcast* sudah sangat umum digunakan pada dunia digital sekarang ini. Saluran TV, radio, *streaming* audio atau pun video lewat internet pun dapat dimasukkan ke dalam media *broadcasting.* Semakain marak digunakannya media ini, maka semakin rentan pula konten yang dapat kita lihat. Konten yang akan dibahas di sini adalah konten yang disiarkan tidak melalui izin dari hak cipta yaitu pemilik dari konten yang bersangkutan.

Agar setiap penyiaran yang dilakukan berisi konten yang sesuai dengan izin hak cipta, maka diperlukan suatu metode untuk membuktikan bahwa konten tersebut yang dapat berupa gambar, suara, atau pun video dimiliki oleh seseorang. Metode yang biasa diapakai adalah metode *watermarking*yang menyisipkan sebuah tanda *copyright* ke dalam konten yang bersangkutan. Proses *watermarking* ini tentunya harus memilki tingkat keamanan yang baik sehingga tidak mudah dimanipulasi oleh pihak yang tidak berwenang, contohnya penyisipan file yang hanya dalam bentuk aslinya dan *visible* dilihat oleh kasat mata akan dapat mudah dimanipulasi oleh perangkat lunak pengolahan *image* yaitu dengan menghapusnya atau menimpanya dengan frame gambar lain. File yang secara umum melewati atau digunakan dalam media *bradcasting* adalah file dalam bentuk digital yang dapat berupa *image*(*banner TV*), *audio*(melalui radio) atau video(melalui saluran TV). Algoritma atau metode yang dapat digunakan adalah dengan metode LSB, spread spectrum. Untuk audio, penyisipan dilakukan pada bit berfrekuensi rendah agar tidak terdeteksi oleh manusia, sedangkan untuk video, penyisipan dilakukan pada matriks pixel untuk setiap frame dari video (suatu video dilihat dari kumpulan *frame image*).

Pengujian akan ditekankan tentang bagaimana menyisipkan suatu file digital ke dalam matriks yang di dapat dari frame tunggal serta bagaimana cara meningkatkan keamanan proses watermarking dari file digital dengan cara melakukan enkripsi menggunakan kombinasi algoritma kriptografi klasik . Metode kritografi klasik yang digunakan pada kali ini adalah metode *affine chipper* dan *vigenere chipper*. Diharapkan kombinasi penggunaan algoritma klasik pada proses watermarking dapat meningkatkan performansi dari segi keamanan.

II. WATERMARK

A. Sejarah Watermark

Pada abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* dengan cara menekan bentuk cetakan gambar pada kertas yang baru setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas yang sudah diberi tanda air ini dijadikan sebagai tanda bahwa karya seni tersebut adalah milik mereka

Sebuah watermark dibuat oleh seseorang dengan menggunakan media karya seni mereka yang dilapisi cap logam selama proses pembuatan karya seni

tersebut. *Watermark* dalam bentuk gulungan diciptakan pada tahun 1826 oleh John Marshall. Watermark juga telah digunakan oleh *papermakers* untuk mengidentifikasi produk mereka, dan juga pada perangko , mata uang , dan dokumen milik pemerintah untuk mencegah adanya pemalsuan .

Di Perancis , mereka diperkenalkan metode *watermark* selama Perang Dunia II . Pada masa tersebut terdapat beberapa kasus pemalsuan dokumen-dokumen dan karya . Penemuan gulungan *watermark* ini merevolusi proses watermark dan membuatnya lebih mudah bagi pemerintah untuk watermark kertas atau dokumen mereka.

Pengertian dari gulungan *watermark* itu sendiri adalah roller ringan yang ditutupi dengan bahan mirip dengan layar jendela kanvas atau kertas yang memiliki pola. garis samar yang dibuat oleh benda semacam kawat atau tali yang berjalan sejajar dengan sumbu dari roll, dan garis tebal yang dibuat dengan kawat yang bersisian di sekitar lingkar kawat untuk mengamankan garis yang diletakkan ke gulungan dari luar.

Tanda timbul ini akan dipindahkan ke *pulp* serat , menekan dan mengurangi ketebalan mereka di daerah itu karena pola dari bagian halaman yang lebih tipisdaripada kertas sekitarnya.

Dalam bidang filateli atau surat menyurat , watermark dulu digunakan sebagai fitur kunci dari perangko, dan seringkali merupakan perbedaan antara umum dan cap langka. Kolektor yang mengalami dua identik perangko dinyatakan dengan tanda air yang berbeda mempertimbangkan cap masing-masing menjadi isu diidentifikasi terpisah. Watermark telah menjadi suatu hal yang umuml pada perangko pada awal abad ke-20 dan 19.

Proses pendeteksian cap watermark pada perangko cukup sederhana. Kadang-kadang sebuah watermark di kertas perangko bisa dilihat hanya dengan melihat sisi belakang. Lebih sering, kolektor harus menggunakan beberapa item dasar untuk melihat yang baik di watermark. Misalnya dengan menggunakan bantuan cairan watermark dapat diterapkan untuk bagian belakang perangko mengekstraksi watermark.

Bahkan dengan menggunakan metode watermarking sederhana yang dijelaskan, bisa sulit untuk membedakan beberapa watermark. Kadang-kadang diperlukan alat khusus untuk melihat watermark seperti detektor watermark Morley-Bright atau Signoscope. Alat tersebut bisa sangat berguna karena dapat digunakan tanpa meneteskan bantuan cairan ekstraksi watermark dan juga memungkinkan kolektor untuk melihat watermark dalam jangka waktu yang lebih lama.

B. Penggunaan Watermark

Watermarking adalah suatu cara atau metode penyisipan atau penanaman data/informasi tertentu ke dalam suatu data digital lainnya dengan maksud mengamankan atau memberi tanda bukti terhadap media tempat penyisipan. Watermark memiliki 2 jenis yaitu watermark *invisible* dan watermark *visible*, adapun watermark *invisible* tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital sampai pada tahap tertentu. Sedangkan watermark *visible* dapat terlihat jelas dan biasanya dimaksudkan hanya sebagai penanda saja.

Watermarking atau tanda air ini sedikit berbeda dengan tanda air yang ada pada uang kertas. Tanda air pada uang kertas masih dapat terlihat oleh kasat mata manusia. Tetapi watermarking yang akan dibahas di sini adalah watermark pada media digital yang dimaksudkan agar tidak dapat dirasakan kehadirannya oleh manusia tanpa alat bantu mesin pengolah digital seperti komputer, dan sejenisnya untuk menyembunyikan tanda hak kepemilikan atau hak cipta dari suatu file digital.

Watermarking yang bersifat *invisible* memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Dengan adanya kekurangan inilah, metoda watermarking dapat diterapkan pada berbagai media digital.

Watermark memiliki berbagai macam tujuan (tidak bermakna sempit hanya dalam perlindungan hak cipta saja). Adapun watermarking dapat dimanfaatkan untuk berbagai tujuan, seperti :

- *Tamper-proofing*; watermarking digunakan sebagai alat untuk mengidentifikasikan atau pembanding yang menunjukkan data telah mengalami perubahan.
- *Feature location*; menggunakan metoda watermarking sebagai alat untuk identifikasikan isi dari data digital pada lokasi-lokasi tertentu.
- *Annotation/caption*; watermarking hanya digunakan sebagai keterangan tentang data digital itu sendiri yang biasanya termasuk ke dalam jenis watermarking yang sifatnya *visible.*
- *Copyright-Labeling*; watermarking dapat digunakan sebagai metoda untuk penyembunyikan label hak cipta pada suatu data digital untuk mencagah adanya penggunaan konten file digital diluar izin contohnya pengguanaan media digital pada *broadcasting*.

Watermarking dalam penerapannya terhadap data digital, dapat diterapkan pada berbagai domain. Maksudnya penerapan watermarking pada data digital seperti teks, citra, video dan audio, dilakukan langsung pada jenis data digital tersebut contohnya pada analisis *spectrum* pada file digital audio, analisis frame pada file digital gambar atau video. Prosesnya dapat juga dilakukan transformasi ke dalam domain yang lain. Berbagai transformasi yang dikenal dalam pemrosesan sinyal digital seperti:

- FFT (Fast Fourier Transform),
- DCT (Discrete Cosine Transform),

- Wavelet Transform.

C. Media *Broadcasting*

Penerapan *watermark* sangatlah luas, salah satu contohnya adalah aplikasi pada media *broadcasting*. *Watermarking* yang digunakan sebagai tanda kepemilikan suatu karya yang dalam dunia *broadcasting* ini berupa file atau pun data digital akan dijadikan identifikasi dan legalitas dari suatu siaran yang di-*broadcast.* Contohnya adalah dalam kasus penyiaran iklan. Pemasang iklan dapat mengetahui apakah iklannya telah ditayangkan sesuai dengan kesepakatan atau tidak. Produser atau pemegang hak milik dari suatu jenis siaran contohnya berupa film akan dapat memonitor distribusi dan penayangan filmnya. Conoth lainnya adalah pada proses survey perhitungan saluran mana yang paling sering ditonton.

sistem watermarking dibagi menjadi tiga tahap yaitu, *embedding*, menyerang dan deteksi. Dalam *embedding*, algoritma menerima host dan data atau informasi di dalamnya dan menghasilkan sinyal watermark untuk ditransmisikan. Jika sinyal yang dikirimkan ini dimodifikasi oleh seseorang,, maka disebut serangan. Seseorang dapat mencoba untuk menghapus watermark digital melalui modifikasi. Ada banyak kemungkinan modifikasi, misalnya, kompresi data, cropping foto atau video, atau dengan menambahkan noise. Deteksi (sering disebut ekstraksi) adalah suatu metode yang digunakan pada sinyal untuk mencoba mengekstrak watermark sinyal tersebut. Jika sinyal tidak dimodifikasi, maka watermark masih dapat diekstraksi. Oleh karena itu, dibutuhkan suatu metode agar watermark pada sinyal susah untuk dimodifikasi oleh orang yang tidak berkepentingan. Salah satu caranya adalah dengan menggunakan kriptografi.

Seperti yang dijelaskan sebelumnya, file digital yang disiarkan melalui media *broadcasting* akan diikuti juga oleh *watermark* atau tanda kepemilikan file tersebut. Untuk meng-ekstraksi tanda hak millik ini dibutuhkan suatu kunci yang hanya produser atau pemilik file tersebut yang mengetahui. Stasiun monitor akan melakukan ekstraksi data dan informasi *watermark* yang ada pada file. Siaran yang illlegal atau yang sudah tidak sesuai izin dari pemilik file akan dapat terdeteksi.

III. METODE

A. Kriptografi Klasik

Kriptografi, secara umum adalah ilmu atau pun metode yang digunakan untuk menjaga kerahasiaan informasi . Informasi pada penerapan abad sekarang adalah informasi data yang berbentuk digital.

Pada bahasan watermarking kali ini, penyisipan data berupa *copyright* atau pun gambar yang menyatakan kepemilikan suatu data atau file digital tidak hanya disisipkan begitu saja, tetapi melalui prinsip enkripsi terlebih dahulu. Enkripsi yang digunakan adalah enkripsi berupa *array* atau matriks dari byte data atau informasi digital yang disisipkan. Alasan penggunaan enkripsi ini adalah jika kunci penyisipan dapat dipecahkan oleh seseorang yang ingin memanipulasi data digital, maka file digital yang berisi bukti kepemilikan tidak dapat langsung digunakan, tetapi harus melewati metode dekripsi kriptografi terlebih dahulu. Diharapkan bahwa penggunaan aplikasi kriptografi pada watermark kali ini dapat meningkatkan performansi dari segi keamanan, walaupun tentu saja penggunaan suatu algoritma kriptografi klasik ini memiliki kelemahan.

Untuk jenis *chipper* yang digunakan pada uji kali ini adalah modifikasi penggabungan affine chipper dengan vigenere chipper.

Affine chipper merupakan perluasan dari chaesar chipper dengan metode sebagai berikut.

Enkripsi: $C \equiv mP + b \pmod{n}$ Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n}$ Kunci: m dan b

Keterangan:

1. n adalah ukuran alfabet
2. m bilangan bulat yang relatif prima dengan n
3. b adalah jumlah pergeseran
4. *Caesar cipher* adalah khusus dari *affine cipher* dengan $m = 1$
5. m^{-1} adalah inversi $m \pmod{n}$, yaitu $m \cdot m^{-1} \equiv 1 \pmod{n}$

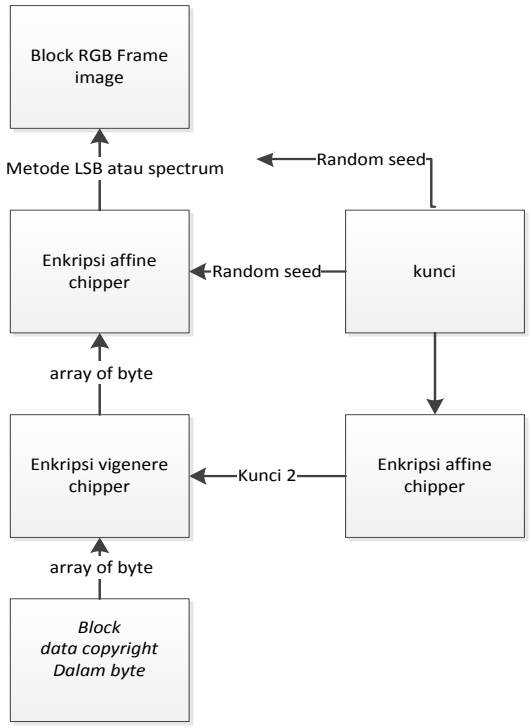
Sedangkan metode dari vigenere chipper adalah sebagai berikut.

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$ Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$ k = kunci rahasia

Modifikasi yang digunakan pada uji kali ini adalah dengan menggabungkan kedua chipper klasik tersebut. Pada affine chipper, kunci yang digunakan adalah 2 yaitu besarnya pergeseran dan bilangan relative prima, sedangkan pada vigenere kunci yang digunakan adalah sebuah deretan karakter atau sebuah string. Pada modifikasi kali ini, kunci yang dimasukkan atau digunakan hanyalah satu saja untuk kedua chipper. Akan digunakan kunci berupa sebuah string, kemudian melalui fungsi *random seed* akan di-*generate* 2 bilangan berbeda(tergantung *seed*) yang digunakan untuk affine chipper. Untuk *affine chipper,* jumlah *range* perpindahan dapat kita tentukan sendiri, pada pengujian digunakan angka 299. Seed adalah nilai penjumlahan karakter dari string kunci. Kunci tersebut tidaklah langsung digunakan untuk melakukan enkripsi vigenere chipper, tetapi kunci yang digunakan merupakan kunci hasil enkripsi dari affine chipper yang nilai 2 bilangan kuncinya di-*generate* oleh string itu sendiri. Kemudian metode atau teknik enkripsi

vigenere dijalankan dengan bersamaan dengan metode affine chipper secara sekuensial pada *array* atau pun matriks yang berisi *byte* dari file digital yang digunakan sebagai pembuktian hak milik (berupa image logo atau teks *copyright*).

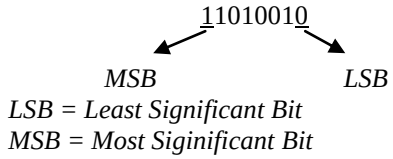
Skema gambar parsial untuk bagian enkripsi dan penyisipan proses watermark dari penjelasan di atas dapat dilihat pada gambar 1.



Gambar 1. Ilustrasi Enkripsi Embedding Watermark

B. Cara Penyisipan

Metode penyisipan pada watermark tidak jauh berbeda dengan metode yang digunakan pada steganografi, Salah satunya adalah dengan mengganti bit *LSB* dengan bit data.



LSB = Least Significant Bit
MSB = Most Siginificant Bit

Mengubah bit *LSB* hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya salah satu kelemahan dari metode ini adalah tidak kokoh terhadap perubahan, mudah dihapus degan mengganti semua bit *LSB* dari media ber-*watermark*.

Metode lain yang dapat digunakan pada proses watermarking adalah metode *spread spectrum*. Metode ini diusulkan pertama kali oleh Cox dalam makalah "*Secure Spread Spectrum Watermarking for Multimedia*" (1997), *Watermark* disebar (*spread*) di dalam citra.

Aplikasi metode *Spread spectrum* dapat dilakukan dalam 2 ranah:

- Ranah spasial
  Menyisipkan *watermark* langsung pada nilai *byte* dari *pixel* citra.
- Ranah *transform*
  Menyisipkan *watermark* pada koefisien transformasi dari citra.

Citra ditransformasi ke dalam ranah frekuensi dengan *DCT* (*Discrete Cosine Transform*). Setelah penyisipan, ranah frekuensi dkembalikan ke ranah spasial dengan *IDCT* (*Inverse Discrete Cosine Transform*). Berikut adalah cara perhitungan DCT dan IDCT.

- DCT:

$$C(p,q) = \alpha_p \alpha_q \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} I(m,n)\cos\frac{\pi(2m+1)p}{2N}\cos\frac{\pi(2n+1)q}{2N}$$

- IDCT:

$$I(m,n) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} \alpha_p \alpha_q C(p,q)\cos\frac{\pi(2m+1)p}{2N}\cos\frac{\pi(2n+1)q}{2N}$$

Pada penerapan media *broadcasting*, penyisipan file informasi pada media seperti video MPEG, media gambar berformat JPEG membutuhkan suatu validasi kompresi file. Berdasarkan batasan masalah, makalah ini hanya menekankan kepada bahasan uji metode enkripsi algoritma klasik

IV. PENGUJIAN ALGORITMA

Pada bagian ini, pengujian akan dilakukan hanya untuk membuktikan valid tidaknya algoritma kombinasi affine chipper dan vigenere chipper yang telah dijelaskan pada bagian III.A. Pengujian mengenai valid tidaknya algoritma ini dilakukan dengan melakukan enkripsi dekripsi pada file teks dan file image yang akan diekstraksi setelah disisipkan pada frame matriks RGB lainnya. Algoritma generasi kunci dan enkripsi kombinasi tertera di bawah.

```
    public static void strToSeed(String
str) {
        int tempSeed = 0;
        char[] inputArray;
        inputArray = str.toCharArray();
        for (int index = 0; index <
inputArray.length; index++) {
            tempSeed += (int)
inputArray[index];
        }

        affine.seed = tempSeed;
```

```
        Random rand1 = new
Random(affine.seed);
        int tempRand1 = rand1.nextInt(12);
        affine.prime = num[tempRand1];
        int tempRand2 = rand1.nextInt(299);
        affine.move = tempRand2;
        affine.key = encrypt26(str);
    }
```

```
    public static String encrypt26(String
str) {
        char[] inputArray;

        inputArray = str.toCharArray();

        for (int index = 0; index <
inputArray.length; index++) {
            char tempinp =
inputArray[index];
            ////enkripsi array of char
            System.out.println((int)
(tempinp - 65));
            int calc = ((prime * (tempinp -
65)) + (move % 26)) % 26;
            System.out.println(calc);
            inputArray[index] = (char)
(calc + 65);

        }
        String output = new
String(inputArray);
        return output;
    }
```

```
public static String encryptAll() {
        char[] inputArray;
        inputArray = input.toCharArray();
        Random rand1 = new Random(move);
        for (int index = 0; index <
inputArray.length; index++) {
            char tempinp =
inputArray[index];
            int tempRand1 =
rand1.nextInt(256);
            int tempMove = move;
            int calc = ((prime * tempinp) +
(tempMove % 256)) % 256;
             if(calc==0){
                calc=256;
            }
            inputArray[index] = (char)
(calc);

        }
        char[] keyArray;
        keyArray = key.toCharArray();

        int idkey = 0;
        for (int index = 0; index <
inputArray.length; index++) {

            char tempinp =
inputArray[index];
            char tempky = keyArray[idkey];
            ////enkripsi array of char
            inputArray[index] = (char)
((tempinp + tempky) % 256);
            idkey++;
```

```
            if (idkey == keyArray.length)
{//reset kunci
                idkey = 0;
            }
        }
        String output = new
String(inputArray);
        int get = (int) inputArray[0];
        return output;
    }
```

A. Uji Enkripsi dan Dekripsi

Berikut adalah contoh plainteks yang digunakan.

Jawa Timur Bakal Tenggelam

Semburan lumpur panas di desa Porong, Sidoarjo, Jawa Timur belum juga berakhir.
Sudah beberapa desa tenggelam. Entah sudah berapa rumah, bangunan, pabrik, dan
sawah yang tenggelam.

Sampai kapan semburan lumpur berhenti, tiada yang tahu. Teknologi manusia tidak
berhasil menutupi lubang semburan. Jika semburan lumpur tidak berhenti juga,
mungkin Jawa Timur akan tenggelam

File plainteks di atas kemudian di enkripsi meggunakan kunci:dimas. Hasil enkripsi dari plainteks tertera di bawah

zz2*ñèÒÄ□w¬%@˜¼ð¯±VK¹¼l£¼û¯ƒ_ÿÝ¦Ä5˜2zÏ_5S þå w¬@¹¼=¯a,ñ˜¦□*ñ¼□ûÄK¹3u • ˜□@å 3u-¼izu›□ûVû_Ç£ó□®ñÚV,*ñ,¦û**ÄÒûùñºà□K¼Ä¯KVÇ £5@Ï¼¬›lð¼¬KI¹þ¹¦¹*@F¯¹□wÇuð˜˜z□_Ç£5@Ï¼¬5□® ¼Ä3u5¼□¼□¹¼□3uÏ¼,5˜˜u¬›@¹ñ¬½□*®wÇu2¼□¼u ûè□¼,V5wþ□_ÿ¬½¦*@□z˜_*w-
@¹ñ=¦Ä5˜2zÏ_5Sþå□w¬…lå £
□,u¬K˜*Ýw¯H*K¹¯□* SIu›èå
Ú£V¹Òu®¼□V□,¼¬K˜K¼å¯umÇ£5□*,Ïóu®è
V aÏ¯¹ Çw ,_,£þK ww □_¿Ïè@_,£þK□ww
u£˜û□åñHÒa**¬…lå £
□,ñÚV,*u¬¯ƒ®˜□¼®,K¬}@□¼¬ë˜®˜2¯@˜¼
¯ VK¹¼l£¼û¯um

File chipperteks di atas kemudian di uji dengan cara di dekripsi balik. Hasil dekripsi balik tertera di bawah.

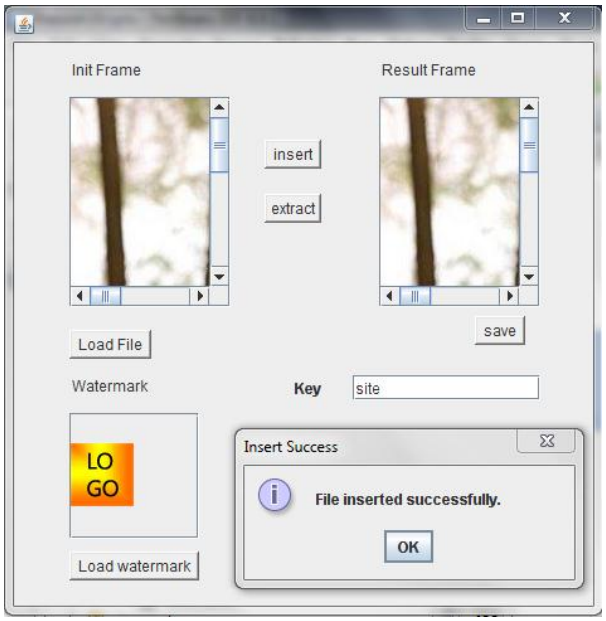
Jawa Timur Bakal Tenggelam

Semburan lumpur panas di desa Porong, Sidoarjo, Jawa Timur belum juga berakhir.
Sudah beberapa desa tenggelam. Entah sudah berapa rumah, bangunan, pabrik, dan
sawah yang tenggelam.

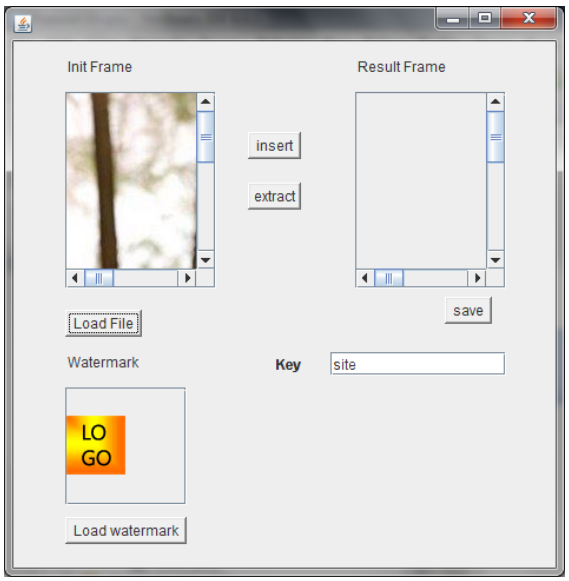
Sampai kapan semburan lumpur berhenti, tiada yang tahu. Teknologi manusia tidak
berhasil menutupi lubang semburan. Jika semburan lumpur tidak berhenti juga,

mungkin Jawa Timur akan tenggelam

Selanjutnya adalah pengujian pada file gambar dengan menyisipkan informasi gambar ke dalam matriks RGB frame lainnya yang disisipkan menggunakan metode LSB 1 bit. Berikut hasil pengujian.



Gambar 2. Uji menyisipkan gambar logo



Gambar 3. Uji ekstraksi gambar logo

B. Hasil

Berdasarkan pengujian di atas, dapat dilihat bahwa algoritma enkripsi dapat digunakan karena skenario pengujian enkripsi dekripsi file teks dan gambar menghasilkan file seperti semula. Walapun pada konsep penerapan enkripsi dan dekripsi pada media *broadcasting* memerlukan pengecekan validasi kompresi, yaitu pada file video ataupun gambar berformat jpeg. Sesuai dengan batasan masalah, pengujian ini memang tidak melakukan uji kepada bagaimana file tempat penyisipan dikompresi atau pun divalidasi sebelum maupun sesudah proses penyisipan.

Pada pengujian, teks dienkripsi menggunakan karakter 256 ASCII dengan kunci "dimas", kemudian dengan menggunakan algoritma dekripsi didapat teks seperti semula. Pada *screenshot* program kecil yang melakukan uji penyisipan suati gambar logo ke dalam frame gambar lainnya, setelah diekstraksi gambar logo didapatkan kembali (menggunakan kunci dekripsi yang sesuai).

Kombinasi *affine chipper* dan *vigenere chipper* ini dari segi kerumitan dan keamanan lebih baik daripada hanya menggunakan *affine chipper*. Pada *affine chipper*, kunci hanya diambil *random* nilai perpindahan dan bilangan relative primanya saja, jadi pada kasus dengan kunci "baba" = 2b + 2a dan "bbaa" = 2b + 2a kemungkinan menghasilkan suatu nilai *seed random* yang sama, namun karena algoritma yang digunakan ditambahkan *vigenere chipper*, maka kasus tersebut dapat diatasi. Kunci yang digunakan pada *vigenere chipper* pun dienkripsi terlebih dahulu menggunakan *affine chipper*, untuk menambahkan nilai kerumitan pada metode enkripsi.

V. KESIMPULAN

Penggunaan algoritma kriptografi klasik secara langsung pada saat sekarang ini sudah banyak ditinggalkan. Telah banyak ditemukan berbagai macam algoritma kriptografi modern yang sudah sangat rumit untuk dipecahkan. Namun, yang perlu kita ingat adalah semua algoritma kriptografi sekarang dapat lahir dari suatu pengembangan dan perbaikan yang ada pada algoritma kriptografi klasik. Kombinasi *generate* kunci pada kombinasi algoritma *affine chipper* dan *vigenere chipper* ini pada dasarnya masih perlu banyak pengujian dan pengembangan. Penggunaan *generate random seed* pada kombinasi algoritma ini dapat menambah performansi dari segi sulitnya pemecahan dan keamanan algoritma.

Dengan mencoba mengimplementasikan kombinasi algoritma kriptografi klasik ini diharapkan kita dapat mengetahui dasar-dasar yang digunakan dalam menerapkan suatu algoritma kriptografi, selain itu dapat melakukan pengembangan dari algoritma kriptografi klasik dilihat dari segi keamanannya untuk digunakan pada berbagai aplikasi modern saat ini contohnya yaitu penggunaan *watermark* pada media *broadcasting.*

REFERENSI

[1] http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/kripto10-11.htm. Diakses tanggal 2 Maret 2011.

[2] http://id.wikipedia.org/wiki/Watermarking Diakses tanggal 19 Maret 2011.

[3] http://en.wikipedia.org/wiki/Digital_watermarking. Diakses tanggal 2 Maret 2011.

[4] http://www.itstudyguide.com
Diakses tanggal 2 Maret 2011.
[5] http://www.scireg.org/english_copyright/infonews_intellectual_property/article_copyright_registration/Digital_watermarking.
Diakses tanggal 21 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, 21 Maret 2011
ttd

Dimas Aditiya Nurahman-13508093