Kriptografi Visual Pada Berkas Video Menggunakan Sebuah Share

Michael Ray / 13517092[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517092@std.stei.itb.ac.id

***Abstract*—Kriptografi visual merupakan sebuah algoritma yang memecahkan sebuah citra tampak menjadi beberapa *share* yang kemudian apabila ditumpuk akan merekonstruksi citra aslinya. Sebuah video merupakan citra tampak juga namun terdiri atas banyak citra tersendiri yang kemudian disatukan untuk menjadi sebuah video. Namun bila digunakan kriptografi visual pada sebuah video, maka *share* hasilnya akan terbentuk untuk setiap *frame* yang ada, dan itu merupakan suatu proses yang berat. Pada makalah ini diajukan sebuah cara agar setiap *frame* pada video memiliki sebuah *share* yang dapat digunakan bersama oleh semua *frame* yang ada pada video untuk merekonstruksi citra asal dari video.**

***Keywords*—Citra tampak, Kriptografi Visual, Share, Video.**

I. PENDAHULUAN

Perkembangan teknologi yang sangat pesat saat ini telah memungkinkan setiap orang untuk menyebarkan informasi secara luas dengan cepat. Perkembangan teknologi juga memungkinkan banyak orang untuk menghasilkan begitu banyak media visual yang tersedia secara luas. Dengan bantuan teknologi internet, semua informasi dan media seakan sangat mudah untuk disebarkan, video yang umumnya memiliki ukuran *file* yang cukup besar dibandingkan dengan *file* lain, tidak ada masalah untuk disediakan dalam jumlah yang banyak di internet. Siapapun dapat dengan mudah menyebarkan apapun di internet. Namun tentunya ada beberapa hal dan informasi yang tidak ingin kita sebarkan secara luas, namun hanya kepada beberapa orang saja. Oleh sebab itu muncullah suatu ilmu untuk menyembunyikan suatu pesan/media dari khalayak ramai dan hanya dapat diakses oleh orang-orang tertentu saja yang disebut kriptografi.

Dalam perkembangan algoritma kriptografi, terdapat banyak jenis algoritma yang tertuju pada beragam tipe media/pesan, salah satu diantaranya adalah kriptografi visual. Kriptografi visual memungkinkan seseorang untuk menyebarkan suatu citra tampak tanpa bisa dikenali dengan cara memecah citra tersebut menjadi beberapa bagian yang disebut *share*, yang kemudian dapat ditumpuk untuk dapat melihat citra aslinya. Pada awalnya kriptografi visual hhanya bisa dilakukan pada citra monokrom saja, namun dengan perkembangan teknologi citra berwarna juga dapat disembunyikan dengan metode ini.

Video juga merupakan salah satu citra tampak yang sedang digunakan untuk mengembangkan algoritma ini. Video merupakan gabungan dari serangkaian gambar diam yang kemudian disatukan untuk menciptakan ilusi dari gambar bergerak. Menggunakan prinsip ini algoritma kriptografi visual tentu dapat diaplikasikan pada sebuah video, namun tentu akan terbentuk begitu banyak *share*.

II. LANDASAN TEORI

A. Kriptografi

Kriptografi (Cryptography) merupakan gabungan dari 2 kata yunani yaitu *cryptos* dan *graphien*, yang berarti *secret* dan *writing*. Pengartian lainnya mengartikan kriptografi sebagai ilmu dan seni untuk menjaga keamanan pesan (Schneier, 1996). Aman pada konteks ini didefiniskan dengan 4 poin yaitu:

1. *Confidentiality*
   Confidentiality atau kerahasiaan dari pesan terjaga dan tidak dapat diakses sembarang orang.
2. *Integrity*
   Integrity atau keaslian pesan terjaga, tidak diubah atau dimanipulasi dengan cara apapun.
3. *Authenticity*
   Authenticity atau keaslian pengirim pesan sehingga dapat dipasstikan bahwa pengirim pesan adalah asli dan bukan pihak lain yang menyamar.
4. *Non-repudiation*
   Non-repudiation atau tidak dapat disangkal maksudnya adalah ketika pesan sudah dikirim, sang pengirim tidak dapat menyangkal bahwa ia telah mengirim pesan tersebut.

Kriptografi pada dasarnya mengandung 2 proses yang saling

terikat satu sama lain, yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana pesan diubah sedemikian rupa sehingga hasilnya tidak dapat dimengerti begitu saja. Namu apabila seseorang memiliki kunci dari proses enkripsi tersebut maka dia dapat melakukan dekripsi, yaitu proses dimana pesan yang sudah diubah kemudian diartikan menjadi pesan yang semula sebelum dienkripsi.

Dalam kriptografi ada 2 tipe yang dibedakan dari kuncinya, yaitu:

1. Algoritma kunci simetris

Algoritma kriptografi kunci simetri, sesuai namanya yaitu algoritma yang kedua belah pihak, baik pengirim maupun penerima memiliki dan mengetahui kunci yang digunakan untuk enkripsi. Dengan begitu algoritma ini menggunakan kunci yang sama untuk kedua proses enkripsi dan dekripsi.

2. Algoritma kunci asimetris

Algoritma kunci asimetris merupakan kebalikan dari kunci simetris, dimana kunci yang digunakan pada proses enkripsi tidak dapat digunakan untuk dekripsi, tetapi ada sebuah kunci lain yang dapat digunakan untuk dekripsi. Dengan begini, sang pengirim memiliki sebuah kunci privat sendiri dan kunci publik miliknya dapat digunakan oleh orang lain untuk mengirim pesan yang hanya bisa ditujukan untuknya.

B. Image

Image atau yang biasa disebut gambar atau citra adalah sebuah representasi dari benda yang digambarkan pada suatu bidang 2 dimensi, sedangkan citra dari sudut pandang matematis merupakan fungsi kontinu dari intensitas cahaya yang terpantulkan dari suatu benda yang kemudian divisualisasikan pada sebuah bidang 2 dimensi. Cahaya yang Sebagian kemudian dipantulkan dari benda yang disinari dapat ditangkap oleh alat-alat optik seperti mata kita atau kamera. Hasil tangkapan cahaya tersebut kemudian direkam dan diterjemahkan pada sebuah kertas agar dapat disimpan.

Citra dapat dikelompokkan menjadi 2, yaitu:

1. Citra tampak

Contoh: Gambar, lukisan, hologram, foto, dll.

2. Citra tidak tampak

Contoh: data yang merepresentasikan sebuah foto dalam file komputer.

Selain citra yang disebut diatas ada pula citra digital, dimana ini merupakan citra yang disimpan dalam bentuk digital dalam komputer. Hanya citra digital lah yang dapat dimanipulasi oleh komputer untuk melakukan enkripsi.

C. Video

Video merupakan suatu contoh dari citra tampak, yang berbentuk sekumpulan gambar yang ditampilkan dengan cepat antar satu sama lain untuk menghasilkan ilusi dimana gambar bisa bergerak.

Suatu video biasanya memiliki suatu angka yang menyatakan jumlah gambar yang ditampilkan per detiknya, atau yang biasa disebut *frames per second* (fps). Rentang dari angka ini sangat bermacam-macam mulai dari 6-9 fps yang biasanya dipakai pada kamera mekanik, hingga yang memiliki 120 frame per detiknya yang ada pada kamera-kamera digital saat ini.

Suatu video dapat ditampilkan menggunakan 2 teknik, yaitu:

1. *Interlaced*

Teknik ini merupakan Teknik yang digunakan pada suatu *raster scanned display device* seperti CRT televisi analog. Teknik ini menampilkan gambar secara bergantian antar garis ganjil dan genap pada layer tampilan secara cepat, dan dilakukan mulai dari atas kiri ke kanan bawah.

2. *Progressive*

Teknik ini merupakan teknik yang sering digunakan pada banyak monitor computer sekarang. Teknik ini menampilkan gambar secara berurutan dan secara langsung pada layar.

Gambar 3. 1 Perbedaan interlaced dan progressive scan

Dengan perkembangan teknologi, sekarang ini muncullah video digital dan sistem perekaman video secara digital juga, dan teknologi video terus berkembang dari yang awalnya perlu disimpan pada sebuah *tape* terlebih dahulu lalu dipindahkan ke *optical disc*, sampai bisa disimpan langsung di *optical disc* tanpa perantara. Hal-hal ini juga memberikan beberapa keuntungan pada video yang dihasilkan dan yang bisa disebarkan, yaitu:

1. Kemampuan untuk disimpan pada media penympanan random seperti magnetic/optical disc.
2. Memungkinkan akses yang cepat pada suatu bagian tertentu dari video.
3. Kualitas video terjaga dan tidak berkurang walau disimpan dalam waktu yang lama.
4. Mempermudah distribusi video.

D. Kriptografi Visual

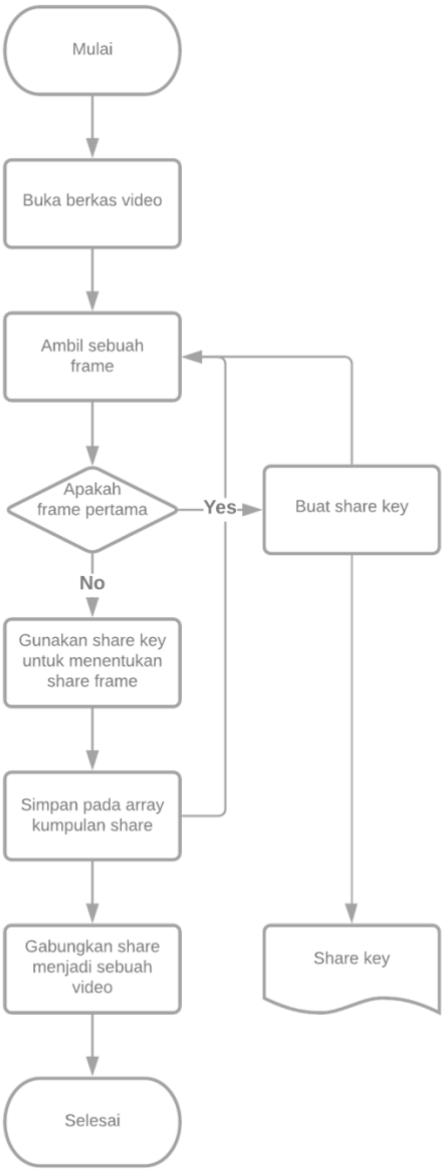
Kriptografi visual merupakan suatu teknik kriptografi yang memanfaatkan indra penglihatan manusia. Kriptografi visual menggunakan teknik yang mengubah suatu informasi visual sedemikian rupa sehingga proses dekripsinya tidak memerlukan komputasi sama sekali.

Teknik yang paling terkenal dalam kriptografi visual adalah teknik yang diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka mendemonstrasikan teknik kriptografi visual dengan cara membagi sebuah gambar menjadi n bagian dimana akan kembali seperti semula jika semua n bagian digabungkan. Namun jika hanya terdapat n-1 saja maka tidak akan tampil gambar asalnya. Masing-masing bagian gambar dicetak pada sebuah plastik transparan dan untuk melakukan dekripsi, yang perlu dilakukan adalah menumpuk semua bagiannya. Teknik ini disebut dengan teknik (N, N) karena membutuhkan n buah bagian untuk melakukan dekripsinya. Kemudian Moni Naor dan Adi Shamir juga memperkenalkan teknik lain dimana hanya memerlukan 2 bagian saja untuk melakukan dekripsinya yaitu teknik (2, N).

Seiring perkembangan yang ada, kriptografi visual sekarang tidak hanya terbatas pada teknik (N, N) saja atau (2, N) namun sekarang sudah dapat dilakukan dengan menggunakan (K, N), dimana k adalah suatu nilai lebih besar dari 2 dan kurang dari n, yang proses dekripsinya membutuhkan k bagian untuk mendapatkan gambar secara sempurna.

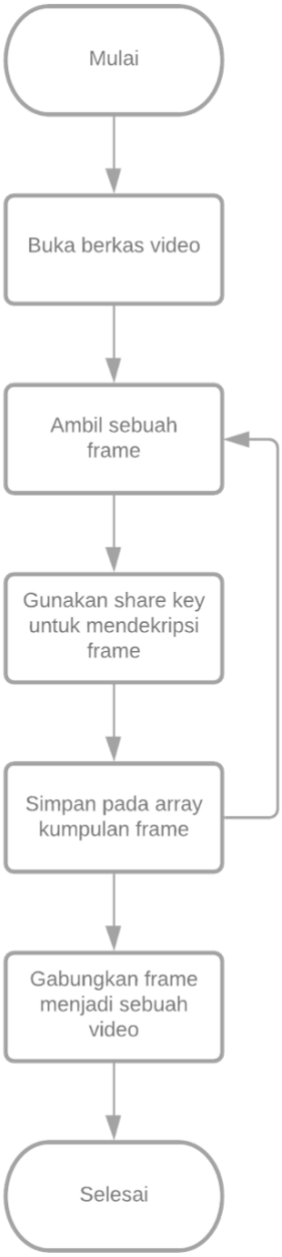
III. IMPLEMENTASI

Untuk mencapai tujuan dari makalah ini, dibentuklah suatu penggambaran visual dari proses yang akan dilakukan terhadap video. Untuk proses enkripsi berikut algoritma yang dibentuk.



Gambar 3.1 Flowchart proses enkripsi video

Sedangkan untuk proses dekripsi adalah sebagai berikut.



Gambar 3.2 Flowchart proses dekripsi

Proses enkripsi pada algoritma yang dibentuk berusaha memperkecil komputasi yang perlu dilakukan dengan cara mengurangi jumlah share yang dibuat. Dengan membuat hanya satu share yang digunakan sebagai *key* oleh semua frame yang ada di video, jumlah share akan berkurang secara drastic dan tentunya mempermudah baik penyimpanan maupun komputasi.

Dengan ide tersebut, berikut merupakan algoritma untuk mengolah sebuah frame:

1. Tentukan dimensi dari gambar (w, dan h).
2. Tentukan nilai k dan n.
3. Hitung nilai recons ((n - k) + 1).
4. Buat array 4 dimensi (n, w, h, 32).
5. Ambil tiap pixel dari frame
6. Translasikan nilai *alpha*, *red*, *green*, dan *blue* ke dalam format 32 bit
7. Untuk frame pertama:
    a. Dengan menggunakan pembangkit bilangan acak, buat sebuah share yang kemudian akan dijadikan key share.
8. Selainnya:
    a. Buat share frame tersebut dengan menggunakan key share sebagai acuan.
9. Masukan hasilnya ke dalam array.
10. Buat array 1 dimensi untuk kemudian menyimpan gambar share per frame.
11. Simpan share ke dalam array.
12. Rekonstruksi gambar dari array 32 bit.

Menggunakan algoritma diatas, dibuatlah sebuah program untuk melakukan analisis.

```
michael22ray21@Michaels-MacBook-Pro Python % python coba.py
============= Visual Kriptografi =============
Main Menu :
1. Encrypt
2. Decrypt
Input : 1
Enkripsi
Masukan nama file video : input.avi
Enkripsi selesai
michael22ray21@Michaels-MacBook-Pro Python %
```

Gambar 3.3 Contoh output proses enkripsi dari program yang dibuat

```
michael22ray21@Michaels-MacBook-Pro Python % python coba.py
============= Visual Kriptografi =============
Main Menu :
1. Encrypt
2. Decrypt
Input : 2
Dekripsi
Masukan nama file video : output.avi
Masukan nama file key share : key.png
Dekripsi selesai
michael22ray21@Michaels-MacBook-Pro Python %
```

Gambar 3.4 Contoh output proses dekripsi dari program yang dibuat

Berikut merupakan contoh hasil *share* dari beberapa *frame* dan *key share*-nya.

Gambar 3.5 Key share yang dibuat oleh program

Gambar 3.6 Share dari frame pertama dari video

Gambar 3.7 Share dari frame ke-20 dari video

IV. Analisis

Tujuan dari makalah ini telah tercapai dengan terbentuknya sebuah video berisi *share* yang berbagi sebuah *share* sebagai *key* dari seluruh video. Video yang terbentuk dari gabungan *share* juga dapat dikembalikan menjadi video awal seperti sedia kala.

Walau proses enkripsi masih tergolong lama terhitung beberapa menit, namun tidak memakan waktu yang terlalu lama jika harus membangkitkan *share* individual untuk setiap *frame*. Perlu diingat juga bahwa video yang dapat dienkripsi oleh program ini masih belum memasuki standar video yang dipakai secara luas, dikarenakan batasan dari kekuatan komputasi, video yang dapat dienkripsi sepertinya masih hanya video dengan jumlah *frame* yang sedikit dan video yang tidak terlalu panjang.

V. Kesimpulan

Kriptografi visual pada video sangatlah memungkinkan untuk dilakukan, namun dengan batasan kekuatan komputasi masih sulit untuk dapat memproses video yang lebih canggih. Mungkin dengan system yang lebih canggih diharapkan dapat mengurangi waktu yang diperlukan dan juga dapat memperluas cakupan video yang bisa diproses.

VII. Acknowledgment

Puji dan syukur saya panjatkan kehadirat Allah SWT. karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan makalah ini tepat waktu. Terima kasih juga saya ucapkan kepada Pak Rinaldi Munir sebagai dosen mata kuliah IF4020 Kriptografi atas ilmu yang diberikan dan diajarkan sehingga dapat saya gunakan pada kesempatan untuk menulis makalah ini.

Referensi

[1] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf

[2] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

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, 3 Desember 2020

Michael Ray / 13517092