

Adaptasi Kriptografi Visual pada Musik

Wiko Putrawan 13509066
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509066@std.stei.itb.ac.id

Abstrak—Kriptografi visual adalah proses enkripsi gambar atau citra yang dilakukan dengan membagi citra menjadi sejumlah bagian. Kriptografi visual dikhususkan untuk enkripsi gambar atau citra. Pada makalah ini, penulis mencoba melakukan adaptasi metode kriptografi visual ini pada musik dengan membagi musik menjadi sejumlah bagian. Musik dapat direpresentasikan ke dalam not balok. Rangkaian not balok tersebut dapat dibagi menjadi beberapa bagian agar pesan yang terdapat dalam not balok tersebut tidak dapat diketahui dengan mudah. Not balok tersebut dapat dibagi berdasarkan instrumen maupun berdasarkan interval tertentu. Hasil pemisahannya dapat diatur sedemikian rupa sehingga tidak mencurigakan jika di dalam lagu tersebut terdapat pesan rahasia.

Kata Kunci—instrumen, interval, kriptografi visual, musik, nada, partitur.

I. PENDAHULUAN

Kriptografi visual diperkenalkan oleh Moni Naor dan Adi Shamir dalam jurnal Eurocrypt '94. Penggunaan kriptografi visual dikhususkan untuk enkripsi gambar atau citra. Enkripsi dilakukan dengan membagi citra menjadi sejumlah bagian (*share*). Kriptografi visual tidak membutuhkan komputasi untuk dekripsi gambar. Proses dekripsi gambar cukup dilakukan menggunakan indera visual manusia. Dekripsi dilakukan dengan menumpuk sejumlah citra bagian.

Musik adalah sebuah bentuk seni dengan medium suara dan keheningan. Elemen-elemen yang ada pada musik adalah *pitch* (yang mengatur melodi dan harmoni), irama (terkait dengan tempo dan artikulasi), dinamika, dan kualitas suara yang dihasilkan. Musik berasal dari bahasa Yunani μουσική (*mousike*, yang artinya *art of the Muses*).

Penciptaan, kinerja, makna, dan definisi musik bervariasi menurut budaya dan konteks sosial. Musik dapat dibagi menjadi genre dan subgenre. Dalam seni, musik dapat diklasifikasikan sebagai seni pertunjukan, seni rupa, dan seni pendengaran. Musik juga dapat dibagi menjadi seni musik dan musik rakyat. Musik juga memiliki hubungan yang kuat dengan matematika. Musik dapat dimainkan atau didengarkan secara langsung, dapat menjadi bagian dari sebuah karyadramatis atau film, atau dapat direkam.

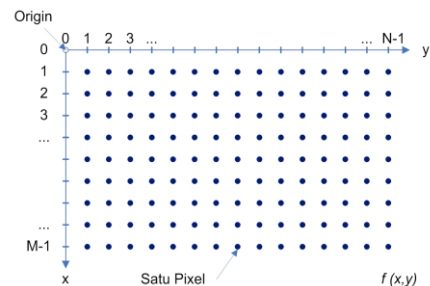
Pada umumnya, sebuah musik terbangun dari permainan beberapa instrumen yang membentuk suatu

kesatuan dan harmoni. Alat musik yang digunakan biasanya terdiri dari alat musik melodi dan alat musik perkusi. Adaptasi kriptografi visual ini dilakukan dengan memisahkan suatu *file* musik yang mengandung sebuah pesan berdasarkan alat-alat musik yang ada di dalamnya.

II. DASAR TEORI

A. Kriptografi Visual

Penggunaan kriptografi visual dikhususkan untuk enkripsi gambar atau citra digital. Citra digital mempunyai definisi fungsi larik dua dimensi $f(x,y)$, di mana x dan y adalah koordinat spasial dan f adalah intensitas warna. Citra digital mempunyai elemen yang disebut *pixel*. *Pixel* adalah elemen pada citra digital yang memiliki lokasi (x, y) dan nilai $f(x,y)$. Nama lain dari pixel adalah *picture elements*, *image elements*, dan *pels*. Representasi citra digital dapat dilihat pada gambar berikut:



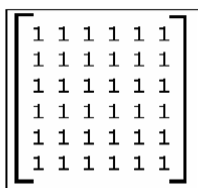
Gambar 1. Representasi citra digital

Citra digital dapat dibagi menjadi tiga bagian, meliputi citra biner (*binary image*), citra abu-abu (*grayscale*), dan citra berwarna.

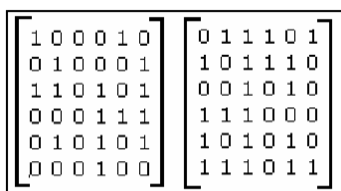
Untuk keamanan, maka dalam kriptografi visual, enkripsi dilakukan oleh pihak ketiga yang terpercaya, yang disebut *dealer*. Sedangkan partisipan ialah orang yang memperoleh citra hasil enkripsi. Dekripsi dilakukan oleh partisipan dengan menumpuk citra yang mereka miliki (citra dicetak pada plastic transparan).

Kriptografi visual memiliki beberapa model, di antaranya model sederhana yang dipaparkan oleh Moni Naor dan Adi Shamir. Citra yang digunakan berupa citra biner, di mana masing-masing *pixel* berwarna hitam atau putih. Dalam pengaplikasiannya, *pixel* akan mengalami

expansion. Masing-masing *pixel* muncul pada *n-share*. Tiap *share* merupakan subset dari citra asli. Contoh kriptografi visual sederhana dapat dilihat pada gambar di bawah, dengan 1 = hitam dan 0 = putih.

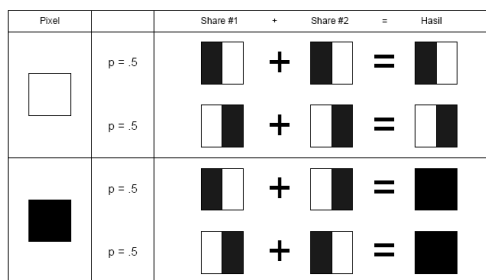


Gambar 2. Model untuk gambar berukuran 6 × 6 berwarna hitam



Gambar 3. Hasil enkripsi Gambar 2

Model di atas sangat sederhana dan tidak aman. Shamir dan Naor mengembangkan model yang lebih baik. Pada model ini, tiap *pixel* tidak direpresentasikan sebagai sebuah elemen matriks pada tiap *share*, melainkan sebagai *m* elemen matriks. Jadi, setiap pixel dibagi menjadi *m* sub-pixel.



Gambar 4. Model kriptografi visual

Dalam model kriptografi visual terdapat istilah skema. Skema ini terdiri dari dua jenis, yaitu skema(n,n) dan skema(k,n). Pada skema(n,n) citra dibagi menjadi *n* buah *share*, di mana untuk mendekripsi citra diperlukan *n* buah *share* tersebut. Pada skema(k,n) citra dibagi menjadi *n* buah *share*, di mana untuk mendekripsi citra diperlukan minimal *k* buah citra hal tersebut. Jika terdapat *q* citra hasil, di mana $q < k$, maka tidak ada informasi apapun yang dapat diperoleh tentang citra asli. Pada pengembangannya, kriptografi visual dapat diterapkan pada citra abu-abu (*grayscale*) dan citra berwarna.

Kelemahan pada kriptografi visual adalah citra hasil dekripsi tidak tepat sama dengan citra asli, citra hasil dekripsi mengandung noise, dan *share* tidak memiliki makna dan dapat menimbulkan kecurigaan bahwa gambar

tersebut merupakan pesan rahasia. Untuk menghilangkan kecurigaan, steganografi digunakan sebagai pelengkap kriptografi. Untuk menghilangkan kecurigaan, digunakan beberapa gambar lain sebagai *cover* untuk menyimpan *share*. Gabungan *share* dan *cover* ini akan menghasilkan kamuflase yang baik.

B. Nada

Nada adalah tinggi rendahnya bunyi dalam lagu, musik, dan sebagainya. Nada juga sering digunakan ketika seseorang berbicara untuk menunjukkan ekspresi yang ingin ia sampaikan. Tinggi rendahnya suatu nada ditentukan oleh frekuensinya. Semakin tinggi nadanya, semakin tinggi pula frekuensi yang dimiliki oleh suara tersebut.

C. Not

Dalam notasi musik, nada dilambangkan oleh not. Sampai saat ini, ada dua cara merepresentasikan suatu not, yaitu not angka dan not balok.

Dalam notasi angka, not ditentukan dengan angka 1 (do), 2 (re), 3 (mi), 4 (fa), 5 (sol), 6 (la), dan 7 (si). Nada 1 tanpa titik merupakan nada C natural di notasi balok. Tanda satu titik di atas not menunjukkan bahwa not tersebut naik satu birama dari nada asli sedangkan tanda satu titik di bawah not menunjukkan bahwa not tersebut turun satu birama dari nada asli.

Kemunculan notasi balok diawali dengan notasi Gregorian. Notasi Gregorian ditemukan oleh Paus Agung Gregori pada tahun 590. Notasi Gregorian adalah awal penulisan musik dengan not balok. Namun pada notasi Gregorian belum ada panjang nada dan masih dengan balok not yang 4 baris. Notasi Gregorian dapat dilihat pada gambar berikut:



Gambar 5 Notasi Gregorian

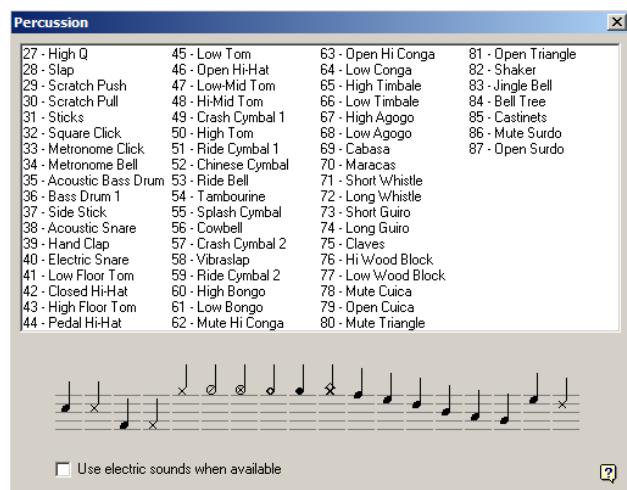
Not balok mempunyai 2 fungsi utama, yang pertama untuk merepresentasikan ketinggian atau interval nada, dan yang kedua sebagai penunjuk nada dalam satuan ketukan. Pembagian not-not dan nilainya dalam ketukan dapat dilihat pada gambar berikut:

bagian, yaitu Percussion (yang berisi alat-alat musik yang dipukul) dan Instrument (yang berisi alat-alat musik selain yang telah termasuk ke dalam Percussion).

Proses pembangunan suatu lagu dilakukan dengan membagi alat-alat musik yang tersedia ke dalam Track. Pembagian alat musik dilakukan berdasarkan kemiripan warna suaranya. Untuk Instrument, alat-alat musik yang ada di dalamnya dibagi menjadi 16 Track, yaitu Pianos, Tuned Idiophones, Organs, Guitars, Bases, String and Timpani, Ensemble String and Voices, Brass, Reeds, Pipes, Synth Leads, Synth Pads, Musical Effects, Ethnics, Percussion, dan Sound Effects. Sedangkan untuk Percussion, hanya ada satu Track yaitu Drum Kit, karena alat-alat musik yang ada pada Track ini hanyalah alat musik perkusi tanpa nada yang hanya memiliki satu frekuensi suara, beda halnya dengan alat-alat musik yang terdapat pada Instrument.

Hanya Track yang terdapat alat musik yang dibutuhkan yang masuk ke dalam properti ketika membuat lagu. Track yang berbeda diaransemen secara terpisah. Ketika lagu tersebut dimainkan, program memainkan Track yang terdapat di dalam properti lagu tersebut secara terpisah dalam waktu yang bersamaan.

Penelitian dalam makalah ini menggunakan fitur Percussion yang terdapat dalam Guitar Pro karena hampir semua alat musik perkusi tanpa nada terdapat dalam fitur ini. Hal ini akan menambah variasi suara dari lagu yang dibangun dan akan menjadi suatu lagu yang dapat dinikmati. Berikut ini adalah daftar 61 alat-alat musik yang terdapat pada Track Percussion dalam Guitar Pro:



Gambar 9 Daftar alat musik yang terdapat pada Track Percussion

Guitar Pro juga dapat melakukan kompresi format dari partitur menjadi MP3 dan sebaliknya. Hal ini tentunya akan mempermudah proses pembuatan cipherteks sesuai dengan yang diinginkan.

B. Finale

Finale tidak jauh berbeda dari Guitar Pro.

Pembendaharaan alat musik di Finale jauh lebih banyak daripada di Guitar Pro. Hanya saja tiap alat musik mempunyai Track-nya masing-masing. Hal ini membuat prosedur penambahan alat musik menjadi lebih rumit.

C. Tool yang digunakan

Penulis menggunakan Finale sebagai tool untuk membuat lagu dalam penelitian kali ini karena Finale mempunyai pemberdaharaan alat musik yang sangat banyak dan dapat digunakan untuk menggabungkan atau memisahkan partitur berdasarkan alat musik yang dimainkan.

IV. IMPLEMENTASI DAN PENGUJIAN

Jika pada citra, kriptografi visual diimplementasikan dengan memisahkan gambar menjadi dua atau lebih gambar sedemikian rupa sehingga gambar awal yang merupakan plainteks tidak dapat dimengerti oleh pihak lain. Namun, cipherteks yang dihasilkan dari pemisahan gambar ini bersifat mencurigakan karena biasanya cipherteks tersebut berupa gambar yang tidak mempunyai arti sama sekali, seperti gambar buram. Agar cipherteks tidak terlalu mencurigakan, cipherteks tersebut dapat digabungkan dengan gambar kamufase, namun masih terdapat noise yang dapat mengundang kecurigaan.

Pada musik, penulis mencoba metode baru untuk menyembunyikan pesan dengan menggunakan adaptasi kriptografi visual pada musik. Sebuah musik terdiri dari not-not yang dapat disisipi pesan. Salah satu penyisipan pesan pada not-not yang ada di dalam suatu musik telah penulis tuliskan dalam makalah yang berjudul "Steganografi pada Musik Tanpa Nada". Dalam makalah ini, penulis mengusulkan dua implementasi adaptasi kriptografi visual pada musik.

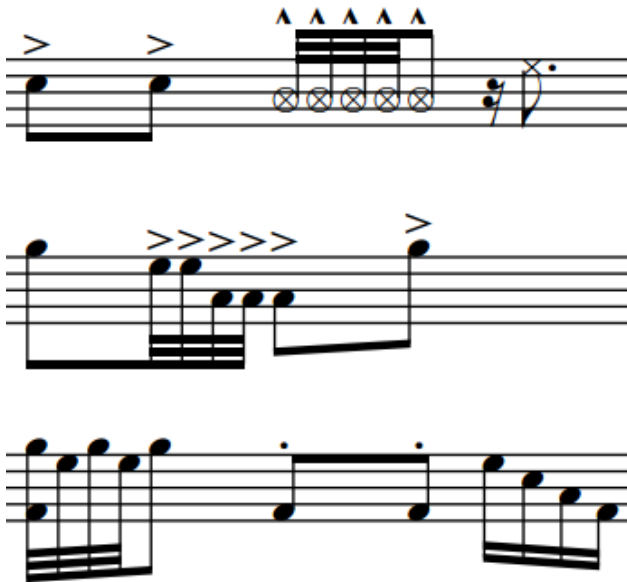
A. Implementasi A

Pada implementasi ini, sebuah pesan disisipkan pada not balok. Penulis menggunakan potongan musik perkusi untuk menyisipkan pesan ke dalamnya. Musik ini memiliki instrumen berupa snare drum, tenor drum, dan bass drum. Berikut ini adalah not balok musik perkusi yang telah disisipkan pesan.



Gambar 10. Cipherteks Implementasi A

Partitur ini kemudian dipisahkan berdasarkan alat musik yang dimainkan dengan menggunakan Finale. Berikut ini adalah hasil pemisahan dari cipherteks.

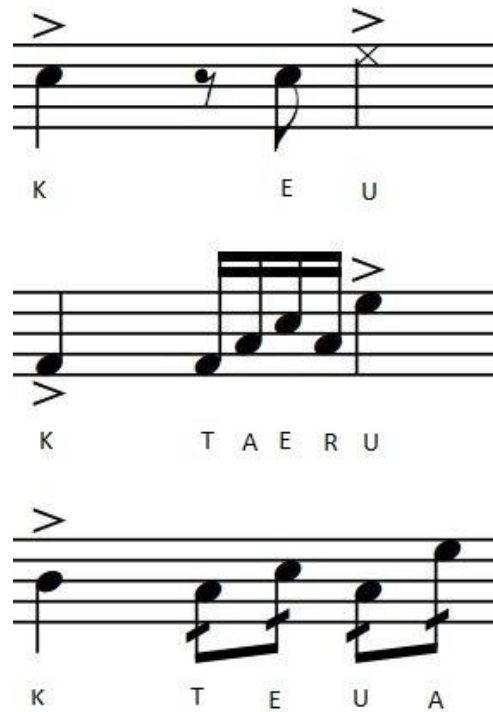


Gambar 11. Hasil pemisahan cipherteks berdasarkan alat musik yang dimainkan

Di mana partitur yang berada paling atas adalah partitur snare drum, partitur yang berada di tengah adalah partitur tenor drum, dan partitur yang berada di paling bawah adalah partitur bass drum. Jika kriptanalis mampu mendekripsi tiga partitur di atas, dia akan menemukan kalimat “UNDIMAJA” pada partitur snare drum, kalimat “UNKAPDJ”, dan kalimat “UJIANDJUKAN” pada partitur bass drum. Hasil dekripsi ini tidak memiliki makna yang berarti dan bahkan dapat membuat kriptanalis salah menebak plainteks yang sesungguhnya. Untuk dapat melakukan dekripsi terhadap cipherteks tersebut, kriptanalis harus mampu menemukan semua *share* dari cipherteks awal, menggabungkan semua *share* yang telah ditemukan, dan melakukan translasi terhadap cipherteks yang telah utuh.

B. Implementasi B

Proses enkripsi yang terjadi pada implementasi ini hampir sama dengan Implementasi A, hanya saja pesan disisipkan ketika partitur sudah dipisahkan berdasarkan alat musik yang ada di dalamnya. Tiap not di-assign kepada satu huruf. Not yang mempunyai posisi yang sama mewakili huruf yang sama. Partitur yang telah disisipkan pesan ini kemudian digabungkan menjadi sebuah musik perkusi. Berikut ini adalah contoh implementasi B dengan menggunakan plainteks “KE UTARA”.



Gambar 12. Cipherteks Implementasi B

Ketiga partitur di atas digabung menjadi satu partitur musik perkusi menggunakan Finale. Hasil penggabungannya adalah sebagai berikut.



Gambar 13. Hasil penggabungan partitur pada Gambar 12

Jika kriptanalis mampu melakukan dekripsi pada Gambar 13, ia akan menemukan kalimat “KATAERUA”. Kata ini tidak memiliki makna yang berarti. Untuk dapat melakukan dekripsi terhadap cipherteks ini, kriptanalis harus memisahkan partitur tersebut berdasarkan alat musik yang dimainkan, melakukan translasi partitur ke dalam huruf, dan menyusun urutan instrumen agar huruf-huruf yang ditemukan dapat membentuk suatu kata atau kalimat yang bermakna.

V. KESIMPULAN

Elemen-elemen musik dapat dijadikan sebagai alat untuk menyembunyikan pesan. Dengan menggunakan teori musik, pesan yang telah disisipkan dapat disamarkan dengan melakukan adaptasi kriptografi visual pada musik. Hasil enkripsinya berupa lagu yang relatif tidak menimbulkan kecurigaan apabila diperdengarkan oleh orang awam. Jika kriptanalis tidak menemukan semua *share* yang dihasilkan, hasil dekripsi dapat berupa kata

atau kalimat yang tidak bermakna bahkan dapat berupa kata atau kalimat yang mempunyai makna yang berbeda dengan plaintexts. Adaptasi kriptografi visual pada musik dapat memfasilitasi penyisipan dan penyamaran pesan tanpa menimbulkan kecurigaan pada ciphertexts yang dihasilkan.

Penggunaan adaptasi kriptografi visual ini dapat dikombinasikan dengan steganografi pada file musik sehingga mempunyai proteksi yang lebih susah untuk ditembus.

VI. ACKNOWLEDGMENT

Penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir, selaku dosen mata kuliah Kriptografi, atas bimbingannya dalam menyusun makalah ini. Tak lupa pula penulis mengucapkan terima kasih kepada segenap anggota Marching Band Waditra Ganesha (MBWG) ITB yang telah membantu penulis mempelajari musik perkusi.

DAFTAR PUSTAKA

- [1] Gary D. Cook, *Teaching Percussion*, p.2, 3rd edn, 2006, Thomson Schirmer, ISBN 0-534-50990-8
- [2] Munir, Rinaldi. 2005. *Kriptografi*. Bandung: Penerbit ITB.
- [3] <http://arisultan.wordpress.com/pengertian-nada-ritme-dan-harmoni-dalam-musik/>, diakses tanggal 5 Maret 2013 pukul 00.32 WIB.
- [4] Taruskin, Richard *The Oxford History of Western Music, Volume 1 - Music from the earliest notations to the 16th century* Chapter 1, the curtain goes up, page 6. (Oxford: Oxford University Press, 2010).
- [5] <http://whiempymusic.blogspot.com/2010/03/membaca-not-balok.html>, diakses tanggal 26 Maret 2013 pukul 03.00 WIB.
- [6] <http://mq.oxfordjournals.org/content/78/3/557.full.pdf+html>, diakses tanggal 26 Maret 2013 pukul 04.15 WIB.
- [7] <http://www.oldenwilde.org/oldenwilde/teaching/musciph.html>, diakses tanggal 26 Maret 2013 pukul 04.16 WIB.

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, 19 Mei 2013



Wiko Putrawan 13509066