APLIKASI STEGANOGRAFI DAN PENERAPAN STEGANALISIS DALAM JIGSAW PUZZLE

Agnes Theresia (13510100)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
agnes.theresia@student.itb.ac.id

***Abstract*— DEWASA ini steganografi didefinisikan sebagai seni menyembunyikan informasi dan data digital di balik informasi digital lainnya dengan cara menyisipkannya di dalam data yang lain. Steganalisis adalah mekanisme untuk memeriksa adanya informasi yang tersembunyi di dalam media stego dan mencegah kerusakan keamanannya. Jigsaw puzzle adalah teka-teki ubi yang memerlukan banyak perakitan kecil, terkadang berbentuk aneh dan saling terkait satu dengan yang lainnya. Ketika selesai disusun, jigsaw puzzle akan menghasilkan gambaran yang utuh. Makalah ini akan membahas steganalisis terhadap informasi yang disimpan di dalam sebuah jigsaw puzzle. Untuk mendeteksi apakah suatu jigsaw puzzle mengandung sebuah informasi lain yang tersembunyi di dalamnya.**

***Index Terms*—steganografi, steganalisis, jigsaw puzzle, informasi tersembunyi.**

I. PENDAHULUAN

Dalam suatu kasus penyampaian informasi kepada beberapa orang tertentu, seseorang perlu melakukan suatu proses yang bertujuan agar orang yang bukan merupakan target tujuan tidak dapat mengerti pesan-pesan yang rahasia yang akan disampaikan. Cara yang dipergunakan dapat beragam. Salah satu cara yang menjadi alternatif adalah enkripsi pesan rahasia yang akan disampaikan. Hal ini dirasakan mampu membuat orang bukan target tujuan tidak dapat membaca pesan rahasia namun pasti membuatnya pasti curiga! Hal ini disebabkan oleh pemakaian bahasa yang terlalu mencolok pada saat proses enkripsi.

Perhatikan perbedaan diantara kedua alternatif ini:

Alternatif 1 :

xjT#9uvmY!rc$

Alternatif 2 :

Lupakan asal rumor itu, jaga agar matamu sehat aku turunkan ubanmu

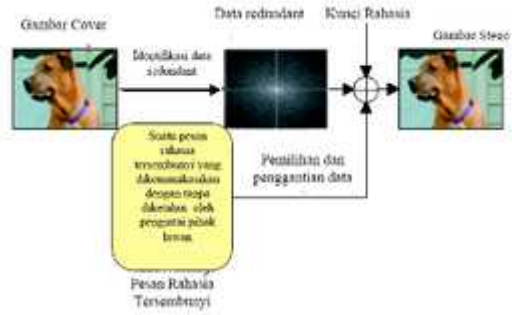
Terjemahan :

Lari jam satu

Manakah pesan yang tidak dan akan menimbulkan kecurigaan? Alternatif 1 adalah hasil dari enkripsi pesan. Karena keluaran pesannya menjadi sangat mencolok, hal ini mengundang kecurigaan orang lain. Sedangkan alternatif 2 adalah cara menyembunyikan pesan di dalam pesan lain. Hal ini bukannya mengundang kecurigaan malahan akan membuat pengertian yang berbeda dari maksud pesan semula dalam pandangan orang bukan target tujuan. Inilah yang disebut menyembunyikan informasi dengan steganografi.

Kata steganografi berasal dari bahasa Yunani steganos yang artinya “tersembunyi atau terselubung” dan graphien “menulis”. Steganografi adalah suatu seni untuk menyembunyikan pesan di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Penyembunyian atau penyamaran pesan ini dilakukan sedemikian rupa sehingga hanya pihak penerima saja yang dapat mengetahui ‘pesan lain’ tersebut. Dalam steganografi pesannya sendiri tetap dipertahankan hanya dalam penyampaiannya disembunyikan dengan berbagai cara. Sangat kecil kemungkinan pesan steganografi untuk dicurigai.

Steganalisis adalah seni dan ilmu untuk mendeteksi pesan tersembunyi menggunakan steganografi , hal ini analog dengan kriptanalisis diterapkan pada kriptografi .



Gambar 1.1 Steganografi pada citra gambar

Kini, istilah steganografi termasuk penyembunyian data digital dalam file-file komputer. Contohnya, si pengirim mulai dengan file gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak

ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam file-file lain yang mengandung teks, image, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Metode ini termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

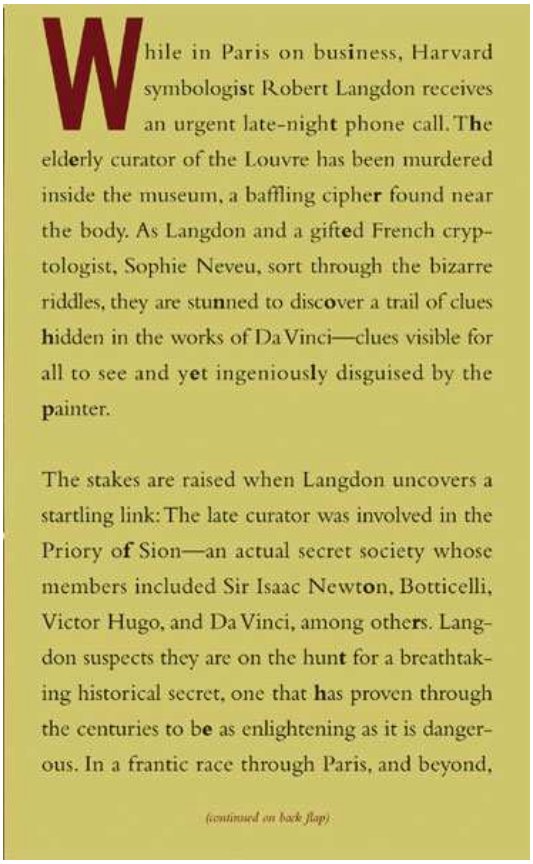
Steganografi digital sering menggunakan berkas-berkas yang ukurannya besar seperti gambar, suara, dan sebagainya. Pada citra gambar, untuk semakin besar tersembunyi yang disembunyikan maka semakin berkurang kualitas media yang dipergunakan sebagai inang. Tetapi hal ini tidak selalu terjadi. Dalam penggunaan teknik steganografi yang tepat dan pengambilan bitnya sesuai, kualitas citra gambar tetap dapat dipertahankan.

II. SEJARAH DAN PENGGUNAAN

A. STEGANOGRAFI

Herodotus adalah seorang sejarawan Yunani pertama yang menulis tentang steganografi, yaitu ketika seorang raja kejam Yunani bernama Histaeus dipenjarakan oleh Raja Darius di Susa pada abad ke-5 sebelum Masehi. Histaeus harus mengirim pesan rahasia kepada anak laki-lakinya, Aristagoras di Militus. Ia menulis pesan dengan cara menato pesan pada kulit kepala seorang budak. Ketika rambut budak itu mulai tumbuh, Histaeus mengutus budak itu ke Militus untuk mengirim pesan dikulit kepalanya tersebut kepada Aristagoras..Masih banyak lagi penerapan steganografi di masa lampau. Semua teknik steganografi konvensional ini selalu berusaha merahasiakan pesan dengan cara menyembunyikan, mengamuflase, ataupun menyamarkan pesan.

Salah satu contoh modern adalah potongan salah satu halaman yang terdapat dalam novel Da Vinci Code oleh Dan Brown.



While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

(continued on back flap)

Gambar 2.1 Contoh Steganografi dalam dunia modern

Sumber gambar: http://www.cert.or.id/~budi/buku-bagus/davincicode.html

Pada tulisan di atas terdapat beberapa kata yang hurufnya sengaja dicetak tebal. Jika huruf-huruf ini dirangkai, maka akan menjadi pesan bermakna. Lebih kurang pesan tersebut adalah "Is there no help for the."

Ada beberapa teknik dalam steganografi, di antaranya adalah:

1. Teknik FLOW (First Letter Of Words)
   Teknik ini sangat sederhana dan tergolong dalam teknik steganografi yang paling efektif. Contoh pemakaian teknik steganografi ini sebagai berikut:

   Umpamanya Sebuah Ember Rusak, Apakah Dapat Menampung Isi Nya. Padahal AdaSeorang Santri, Akan Datang Meminta Isi Nya.

   Jika kalimat di atas diurai dengan teknik FLOW, akan menghasilkan pesan sebagai berikut:
   user admin pass admin

2. Teknik LSB
   Teknik ini juga cukup terkenal. Teknik ini lebih sering diterapkan pada file multimedia seperti file gambar, file audio atau file video. Cara kerjanya adalah mengubah bit terakhir dari masing-masing Byte data. Misalnya media yang digunakan memiliki susunan bit sebagai berikut:

00111101 00110101 01001100 00110100
00111101 00110101 01001100 00110100

Misalnya kita mau menyisipkan "A" asciinya adalah 65 yang binernya adalah : 01000001
Teknik penyisipannya sebagai berikut:

00111100 00110101 01001100 00110100
00111100 00110100 01001100 00110101

3. Teknik White Space
   Teknik ini hampir sama dengan teknik LSB, hanya saja pada teknik White Space ini memanfaatkan Spasi dan Tab sebagai sisipannya. Misalnya ada huruf "A" (mau disisipkan pada kalimat:

   Saya Segera Datang Ke Tempatmu Sendiri Jam 10.

   Dalam teknik ini biner dari pesan yang akan disisipkan akan ditaruh di spasi atau tab dari medianya. 0 direpresentasikan dengan spasi sedangkan 1 direpresentasikan dengan tab.

   Saya Segera Datang Ke Tempatmu Sendiri Jam 10
   .
   0 1 0 0 0 0 0 1

4. Teknik EOF
   Teknik EOF ini menyisipkan pesan pada akhir file. Teknik ini lumayan bagus karena ukuran pesan yang bisa disisipkan tergantung pada kemauan kita sesuai dengan pesan yang disisipkan. Ukuran akhir dari file=ukuran awal file + ukuran pesan.

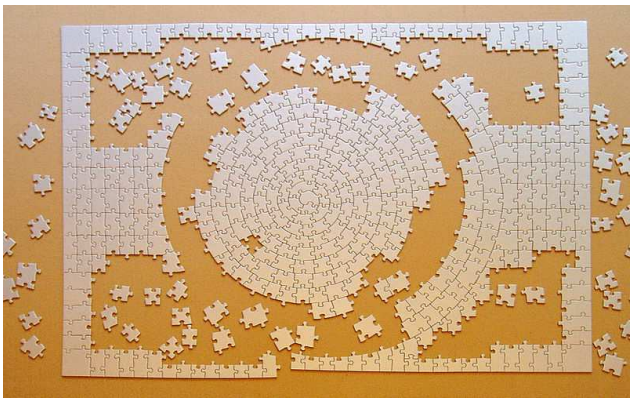
B. STEGANALISIS

Tujuan dari steganalisis adalah untuk mengidentifikasi paket yang dicurigai, menentukan apakah memiliki atau tidak memiliki muatan yang dikodekan didalamnya dan, jika mungkin, membongkar kembali muatan itu. Berbeda dengan kriptanalisis yang jelas bahwa data dicegat berisi pesan (meskipun pesan yang dienkripsi), steganalisis umumnya dimulai dengan tumpukan file data tersangka, tapi sedikit informasi tentang file, yang mana yang mengandung muatan informasi tersembunyi. Bahkan ada kemungkinan tidak ada file yang berisikan muatan tersebut.

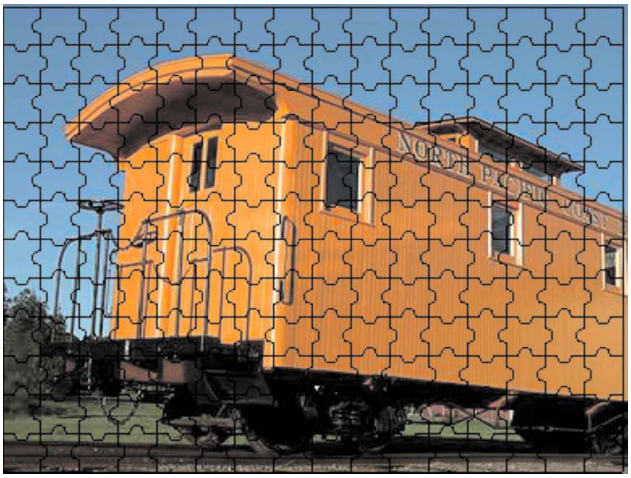
Peristiwa di mana mendeteksi file yang dicurigai menjadi sangat mudah adalah ketika terdapat file asli, belum dimodifikasi, yang tersedia untuk dipakai sebagai pembanding. Membandingkan file paket terhadap file asli akan menunjukkan perbedaan yang disebabkan oleh *encoding payload* dan dengan demikian muatan yang berisi informasi tersembunyi dapat diekstraksi.

C. JIGSAW PUZZLE

Jigsaw puzzle pada awalnya diciptakan dengan membuat gambar pada sepotong kayu datar yang berbentuk lalu gambar tersebut dipotong menjadi potongan-potongan kecil dengan gergaji, Kemudian nama John Spilsbury , seorang pembuat peta dan pemahat dari London, dikenal karena jigsaw puzzle-nya sejak tahun 1760. Lalu jigsaw puzzle mulai dibuat dari karton. Menyembunyikan informasi di dalam jigsaw puzzle cukup banyak dilakukan.



Gambar 2.2 Jigsaw Puzzle yang tidak berupa gambar

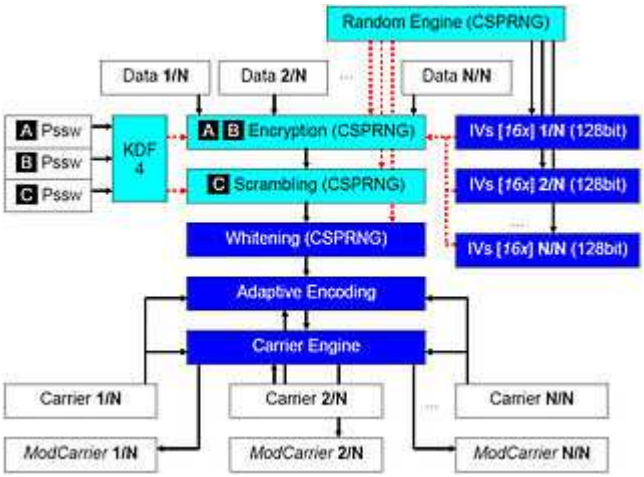


Gambar 2.3 Jigsaw Puzzle utuh yang menampilkan gambar

Dari kedua gambar di atas, dapat kita amati bahwa garis-garis yang memisahkan potongan-potongan puzzle berupa garis hitam dan putih. Kenyataan bahwa banyaknya situs dunia maya yang menampilkan jigsaw puzzle di halamannya membuat beberapa orang tergerak untuk menyimpan berbagai informasi di dalamnya.

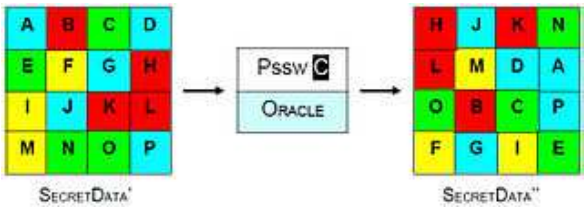
III. ANALISIS

Di bawah ini adalah arsitektur steganografi:

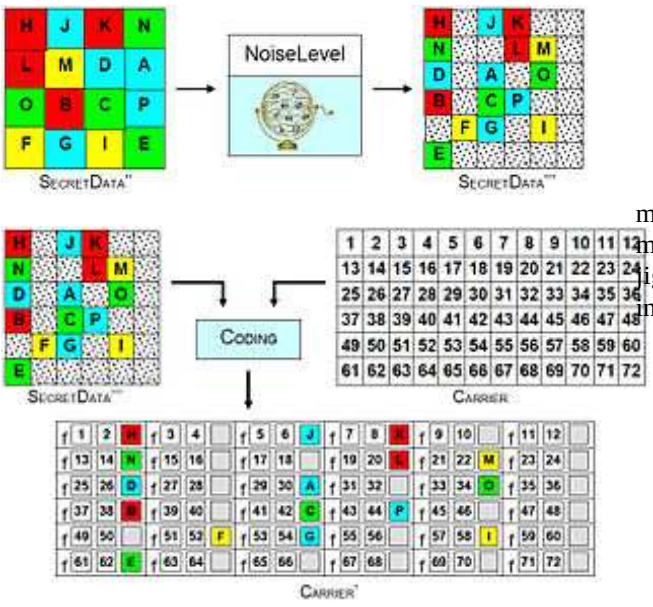


Perangkat lunak steganografi menerapkan subset dari proses steganografi digital yang paling umum sehingga memungkinkan pengguna memasukkan dan mengekstrak data yang disembunyikan dari dan ke file pembawa.

Tujuan menggunakan perangkat steganografi ini adalah untuk menjamin data yang akan disembunyikan bersifat sangat rahasia dan tidak tampak. Perangkat steganografi juga dapat menampilkan hasil kriptografi pada data yang tersembunyi namun ini bukan suatu hal yang pasti terjadi, yang pasti terjadi pertama kali adalah data yang disembunyikan akan menjadi tidak tampak (*invisible*).



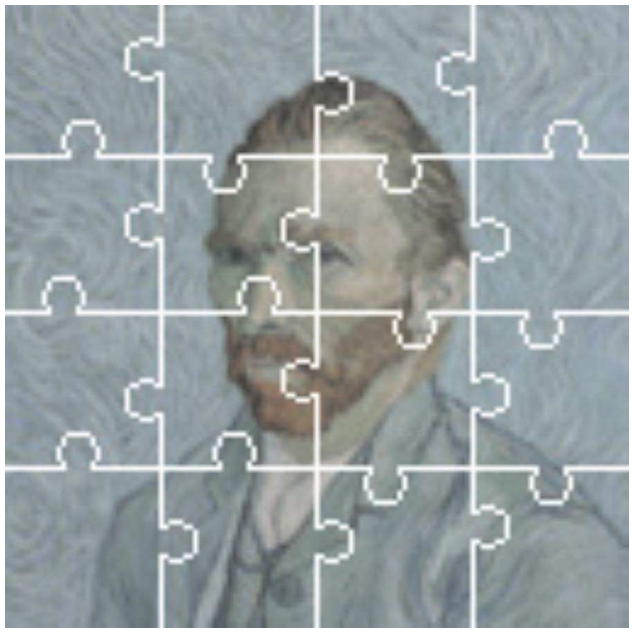
Biasanya data yang secara rahasia dikomunikasikan adalah data yang akan disembunyikan, steganografi berfokus pada data yang seperti ini.



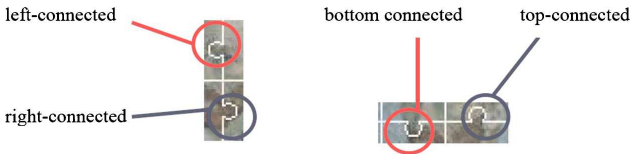
Di atas ini adalah gambar proses encoding data yang akan disembunyikan.

Dalam proses steganografi terdapat beberapa perlindungan terhadap embedding data yang akan disembunyikan.

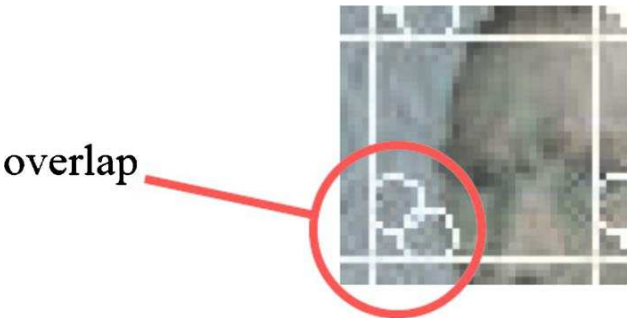
Sebelum menunjukkan bagaimana suatu jigsaw puzzle yang mengandung data di dalamnya, ada baiknya kita memperhatikan gambar jigsaw puzzle di bawah ini.



Ini adalah gambar utuh suatu jigsaw puzzle yang telah disusun dengan tepat. Data yang ingin disembunyikan biasanya di-*embed* pada lekuk yang terdapat di keempat sisi setiap potongan jigsaw puzzle. Setiap lekuk yang berbeda menyimpan informasi yang berbeda pula, karena itu sangat diperlukan keberhati-hatian dalam men-steganalisis potongan jigsaw puzzle ini.



Gambar di atas ini menunjukkan keempat tipe dari masing-masing sisi suatu potongan jigsaw puzzle. Dengan memilih satu atau dua dari keempat sisi suatu potongan jigsaw kita bisa memeriksa tempat dimana kira-kira informasi disimpan.



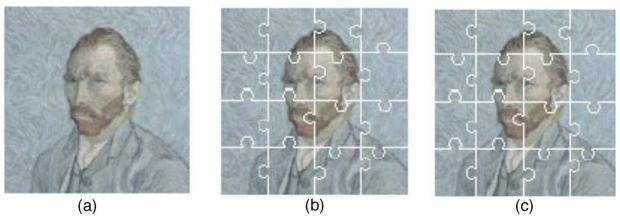
Dalam proses embedding informasi, sangat perlu untuk mengatur jari-jari dari lekuk sisi agar tidak terjadi overlapping seperti yang terlihat pada gambar di atas. Hal ini bertujuan agar steganografi tidak dengan mudah dipecahkan oleh bukan target yang dituju.
Dalam menetapkan ukuran jari-jari yang tepat, dipergunakan rumusan:

Untuk ukuran nxn suatu potongan jigsaw puzzle, posisi pixel yang hendak disisipkan pada sisi salah satu potongan berada pada posisi 0 sampai n-1 dan posisi lekukan berada pada P dimana P adalah elemen dari [3r, n-3r] setelah tadi disepakati bahwa besar r (jari-jari lekukan tidak boleh lebih dari 3).
Dengan demikian kita memiliki (n-6r)+1 posisi berbeda yang bisa digunakan untuk meng-*embed* informasi dengan setiap lekuk mewakili 1 bit informasi. Hal ini menunjukkan kapasitas *embedding*dari setiap potongan puzzle adalah paling sedikit $\log_2 (n-6r)+1$ bits

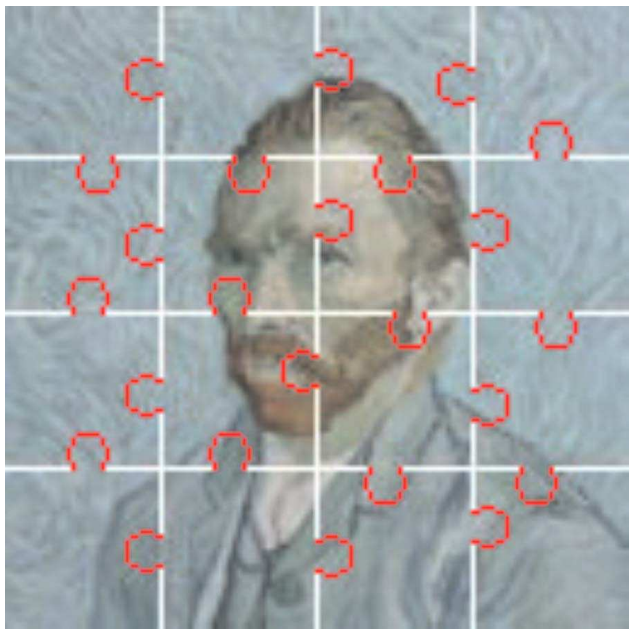
Posisi yang bisa ditempati menjadi:
s' = (t+s)mod(n-6r)

P =
{
(s' + 3r jika sisi potongan adalah IS dan s'<1)
(s'+ 3r + 1 jika sisi potongan adalah suatu IS dan s' ≥ t)
(t+3r jika sisi potongan adalah suatu DS)
}

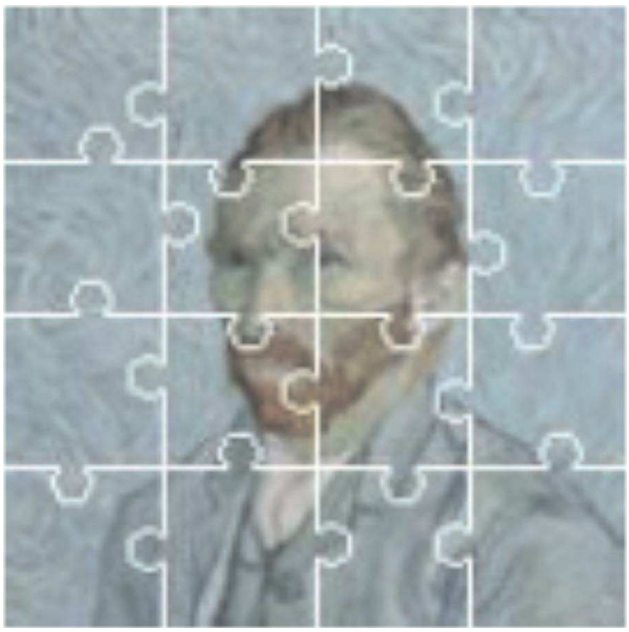
dimana DS adalah Dummy Side (tidak ada data yang di-*embed*), IS adalah Information Side (terdapat data di dalamnya), s adalah data yang tersembunyi untuk k bits dengan k = $[\log_2 (n-6r)+1]$ dan t elemen dari [0, n-6r].



Gambar (a) image original (b) jigsaw puzzle image dengan data embedded (c) versi compressed dari (b)



Di atas ini adalah hasil gambar utuh dari ekstraksi jigsaw puzzle yang sebelumnya dengan lekukan diberikan warna merah. Bandingkan dengan gambar di bawah ini yang merupakan gambar utuh tanpa mengandung informasi apapun di dalamnya. (Tidak mengandung data embedded)



Sangat sulit dibedakan bukan?

V. KESIMPULAN

Jigsaw puzzle hanya salah satu dari sekian banyak media yang dapat digunakan sebagai penyimpanan informasi. Kita tidak akan dapat membedakan manakah media yang mengandung suatu informasi di dalamnya atau manakah media yang benar-benar kosong. Steganalisis merupakan suatu metode yang tergolong cukup baik dalam melakukan penyimpanan informasi di dalam suatu media yang berbeda. Hanya dengan melakukan sederetan mekanisme stegnalisis, kita bisa mengetahui apakah di

dalam suatu gambar/video/jigsaw puzzle terkandung suatu informasi. Hal ini cukup sebanding dengan perjuangan untuk melakukan penyimpanan data yang tidak bisa dikatakan mudah. Namun bila kita menggunakan perangkat Steganografi yang telah disebutkan di atas juga, hal peng-*embed* dan peng-*extract* bukanlah sesuatu yang sangat sulit.

DAFTAR PUSTAKA

[1] http://en.wikipedia.org/wiki/Steganography_tools#Hidden_data (diakses tanggal 11 Desember 2011 pukul 22.30 WIB)

[2] http://www.cs.nthu.edu.tw/~cchen/Research/2009OE.pdf (diakses tanggal 11 Desember 2011 pukul 23.00 WIB)

[3] http://www.mendeley.com/research/steganography-menggunakan-teknik-lsb-pada/# (diakses tanggal 11 Desember 2011 pukul 16.00 WIB)

[4] http://www.kaskus.us/showthread.php?t=3995252 (diakses tanggal 11 Desember 2011 pukul 15.00 WIB)

[5] http://andiktaufiq.wordpress.com/2010/11/19/belajar-steganografi/ (diakses tanggal 11 Desember 2011 pukul 16.30 WIB)

[6] Steganografi.ppt (diakses tanggal 11 Desember 2011 pukul 10.00 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, 12 Desember 2011

ttd

Agnes Theresia
13510100