Studi dan Eksperimen Kombinasi Kriptografi Visual dan Aspek Steganografi
IF3058 Kriptografi

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

***Abstrak*--Kriptografi visual merupakan satu alternatif dalam aspek kriptografi yang memanfaatkan suatu metode yang memungkinkan suatu plainteks dapat dihasilkan secara visual dengan hanya menggabungkan cipherteks dan kunci. Cipherteks dan kunci yang dihasilkan merupakan dua hal yang dipisahkan dari plainteks secara visual. Secara sederhana, plaimteks dapat dihasilkan dengan menumpukkan cipherteks dan transparansi (kunci) yang bersesuaian. Pengamanan menggunakan metode tersebut membutuhkan komunikasi terpisah untuk cipherteks maupun transparansi. Keterpisahan tersebut tidak menjamin ketersampaian transparansi pada pihak berkepentingan. Oleh karena itu, dibutuhkan metode penyembunyian dengan konsep steganografi. Penyembunyian tersebut menyatukan transparansi dan cipherteks sehingga keduanya dapat dikirim secara bersamaan dan diekstraksi melalui metode tertentu.**

***Kata kunci*--kriptografi visual, steganografi, transparansi.**

I. PENDAHULUAN

Kriptografi visual merupakan suatu kajian mengenai pengamanan terhadap materi-materi visual melalui suatu teknik enkripsi yang pendekripsianya dapat dilakukan secara sederhana menggunakan kemampuan penglihatan manusia. Secara teknis sederhana, pada enkripsi kriptografi visual, sebuah berkas dipisahkan menjadi dua model yang terdiri dari "cipherteks" dan transparansi. Kedua model tersebut pada mulanya hanyalah berupa pemisahan antara pixel-pixel dengan warna dan kecerahan yang berbeda. Model "cipherteks" yang dihasilkan melalui metode kriptografi visual merupakan materi yang dapat didistribusikan (dikirim ke pihak yang berkepentingan). Di sisi lain, transparansi merupakan kunci rahasia yang digunakan untuk membuka "cipherteks". Plainteks berupa gambar dapat dibuka kembali apabila cipherteks dikombinasikan dengan transparansi.

Kriptografi visual adalah salah satu metode kriptografi modern yang menerapkan aspek keamanan kriptografi klasik *one time-pad.* Hal tersebut dapat dilihat dari penggunaan cipherteks dan transparansi sebagaimana penggunaan "kamus" untuk mendekripsi cipherteks hasil enkripsi metode *one time-pad*. Oleh karenanya, hanya pihak yang memiliki transparansilah yang dapat membuka plainteks yang dienkripsi menggunakan metode kriptografi visual.

Satu-satunya kelemahan dari *one time-pad* adalah apabila kamus yang digunakan untuk mendekripsi didapatkan oleh pihak yang tidak berkepentingan sehingga metode dekripsi-enkripsi dapat dipecahkan dengan mudah. Akuisisi kamus tersebut dapat dilakukan melalui distribusi kamus yang disadap pihak tidak berkepentingan.

Salah satu solusi yang ditawarkan adalah metode penyembunyian transparansi melalui teknik steganografi. Steganografi merupakan suatu kajian mengenai metode penyembunyian pesan pada materi lain yang tampak lebih signifikan sehingga pesan asli tidak terlihat penting. Melalui penyembunyian tersebut, solusi ini meningkatkan keterjaminan pada keamanan pesan.

II. DASAR TEORI

A. Kriptografi Visual

Kriptografi merupakan penggabungan dari dua kata dalam bahasa yunani, yaitu *kryptos* yang berarti menyembunyikan dan *graphien* yang berarti menulis. Secara terminologi dapat diartikan sebagai teknik dan

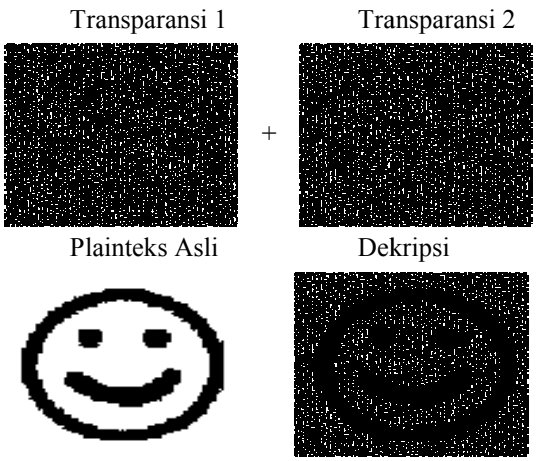
ilmu menyembunyikan pesan tertulis sebagai sesuatu yang tidak dapat dibaca.

Kriptografi memiliki beberapa aspek dalam penyedian keamanannya. Aspek-aspek tersebut yaitu:

1. *Confidentiality,* aspek keterjagaan isi pesan dari keterbukaannya bagi pihak-pihak yang tidak berkepentingan.
2. *Data Integrity*, aspek jaminan keutuhan pesan tanpa adanya manipulasi dalam transmisinya.
3. *Authentication,* aspek identifikasi kebenaran pihak yang terlibat dalam komunikasi.
4. *Non-repudiation*, aspek pencegahan pihak terkait melakukan penyangkalan terhadap pesan yang ditransmisikan.

Salah satu teknologi yang berkembang dalam kriptografi adalah kriptografi visual. Metode ini diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam jurnal *Eurocrypt '94*. Metode kriptografi ini awalnya dikhususkan untuk enkripsi gambar dengan membaginya menjadi beberapa bagian yang disebut sebagai *share*.

Satu aspek keunikan pada kriptografi visual adalah bahwa proses dekripsi tidak membutuhkan komputasi yang rumit. Hal tersebut cukup dengan menumpuk sejumlah citra bagian dan dengannya akan muncul secara visual, suatu citra yang pada awalnya terenkripsi menggunakan metode ini. Sebagai contoh, penerapan metode kriptografi visual dapat dilihat pada gambar berikut.



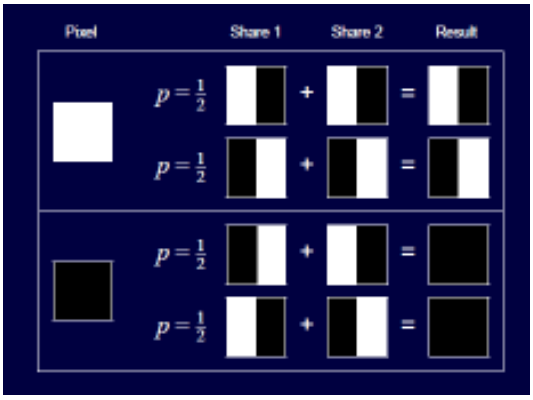
Contoh Kriptografi Visual

Terlihat pada gambar tersebut bahwa *share-share* hasil enkripsi melalui metode kriptografi visual menghasilkan gambar yang serupa dengan plainteks asli apabila ditumpuk. Akan tetapi, dapat terlihat pula bahwa hasil dekripsi menunjukkan gambar yang "terganggu". Hal tersebut disebabkan adanya *noise* yang diakibatkan dari metode enkripsinya.

Penanganan sederhana dari kriptografi visual adalah dengan menggunakan representasi gambar *binary*. Hal tersebut berarti gambar yang digunakan berupa citra hitam-putih sederhana. Citra tersebut ditangani pixel-nya secara terpisah. Pixel tersebut disimpan dalam sejumlah *share* yang merupakan sejumlah kumpulan sub-pixel hitam-putih.

Sub-pixel yang disimpan tersebut dicetak secara berdekatan sehingga dipandang rata distribusinya dengan sistem penglihatan manusia. Representasi dari *share* tersebut dapat dilihat sebagai matriks *Boolean S* berukuran *axb* dengan *a* adalah jumlah *share* dan *b* adalah jumlah sub-pixel pada *share* tersebut.

Pada representasi matriks tersebut, *S[i,j]* bernilai 1 apabila sub-pixel *j* pada *share* ke-*i* berwarna hitam. Sebaliknya, sel matriks tersebut bernilai 0 apabila sub-pixel pada posisi yang sama berwarna putih. Dapat dilihat dari representasi matriks tersebut bahwa banyaknya baris menyatakan jumlah sub-pixel dan banyaknya kolom menyatakan jumlah sub-pixel yang disimpan. Representasi *share* dapat dilihat pada gambar berikut.



Representasi *share*

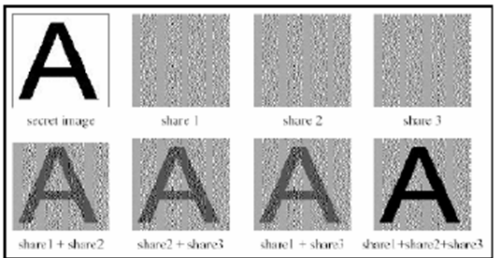
Dapat dilihat juga pada gambar di atas bahwa dekripsi dari *share-share* yang dibangun melalui metode kriptografi visual pada dasarnya adalah operasi logika OR terhadap baris-baris yang bersesuaian pada *share-share* yang dihimpunkan.

Melalui pengoperasian tersebut, warna hitam tidak dapat dihilangkan dengan warna putih yang bertumpuk. Oleh karenanya sebuah penghitungan bobot dipergunakan untuk menentukan apabila suatu share berwarna hitam maupun putih. Penghitungan bobot tersebut dikenal sebagai penghitungan Bobot Hamming [*H(V)*] yang memanfaatkan nilai *Boolean V* dari matriks *S* yang telah didefinisikan dan suatu nilai *d* yang telah ditentukan. Penghitungan dilakukan dengan ketentuan:

- Dianggap berwarna hitam bila *H(V)* melebihi nilai batas *d.*
- Dianggap berwarna putih bila *H(V)* kurang dari nilai $d - (\alpha * m)$ dengan $\alpha > 0$.

Selain dari pendekatan pemisahan *share* untuk sub-pixel, terdapat dua skema dalam merancang transparansi pada kriptografi visual:

1. Skema (n,n); skema ini menghasilkan sejumlah transparansi yang semuanya harus disatukan untuk menghasilkan citra plainteks.
2. Skema (k,n); skema ini menghasilkan beberapa transparansi yang membutuhkan sejumlah *k* transparansi tersebut untuk membuka citra plainteks



Skema (2,3) kriptografi visual, plainteks dapat dilihat menggunakan 2 dari 3 transparansi tersedia.

B. Steganografi Citra Visual

Kata steganografi merupakan agregat dari dua kata dalam bahasa yunani: *steganos* yang berarti terlindungi/tertutupi dan *graphien* yang berarti menulis. Secara terminologi kata ini berarti teknik dan ilmu mengenai penyembunyian pesan dalam suatu pesan lainnya. Pada hakikatnya, steganografi dan kriptografi berada pada kajian yang relatif terpisah. Hal ini disebabkan pada dasarnya kriptografi adalah suatu metode untuk membuyarkan isi pesan sehingga tidak dapat dibaca, sedangkan steganografi adalah metode untuk menyembunyikan pesan pada objek lain sehingga pesan asli dianggap tidak penting. Meskipun demikian, steganografi pada umumnya dipandang sebagai ekstensi dari pengamanan yang diberlakukan melalui metode-metode kriptografi.

Elemen-elemen yang dibutuhkan sehingga dapat dibentuk suatu teks steganografi adalah:

- *Embedded message*, yaitu pesan yang disembunyikan.
- *Cover-object*, yaitu objek yang digunakan untuk menyembunyikan *embedded object*.
- *Stego-object,* yaitu objek yang sudah berisi *embedded message*.
- *Stego-key*, yaitu kunci yang digunakan untuk mengekstraksi pesan.

Contoh yang umum digunakan dalam implementasi tersebut tercakup pada suatu skenario *prisoner's problem.* Pada skenario tersebut, dua orang yang berperan sebagai tawanan saling berkomunikasi merencanakan pelarian. Akan tetapi, kedua pihak terpisah jauh dan mengetahui bahwa pesan yang mereka kirimkan akan dibaca terlebih dahulu oleh penjaga. Oleh karenanya, suatu penyembunyian pesan dilakukan sehingga pihak *eavesdropper* menganggap pesan yang dikirimkan terlihat tidak penting dan tidak mencurigakan.

Salah satu hal yang dapat dicontohkan dalam skenario tawanan tersebut adalah melakukan penempatan pesan utama pada suatu *stego-object* berupa teks yang berbunyi "lamunan agar rumah ibu jadi agak menarik sehingga anak tidak ubanan." Apabila kedua pihak mengetahui bahwa *stego-key* yang digunakan adalah *pembacaan huruf awal kata*, maka kedua pihak akan mengerti bahwa pesan

tersebut merupakan pesan yang terdiri dari *embedded message* yang berbunyi "lari jam satu" dan disembunyikan dalam *cover-object* berupa teks berbunyi "amunan gar umah bu adi gak enarik ehingga nak idak banan." Pesan yang dikirimkan dalam *stego-object* tersebut tampak tidak mencurigakan meskipun berisi suatu pesan yang penting.

Pada dasarnya, teknik steganografi dapat diberlakukan dalam berkas manapun apabila digabungkan dengan teknologi digitisasi yang ada pada saat ini. Suatu data direpresentasikan dalam rangkaian bit yang dapat ditentukan posisi *least significant*-nya. Posisi ini menunjukkan bahwa apabila data berbentuk bit diubah pada posisi tersebut, maka hal itu tidak akan mempengaruhi data utama secara signifikan.

Pada dasarnya, citra gambar yang didigitisasi pada komputer merupakan serangkaian data yang direpresentasikan pada *array*. Data tersebut direpresentasikan sebagai sesuatu yang dikenal dengan nama pixel. Setiap pixel diwakili posisi fisiknya dengan posisi logik pada *array* tersebut dan ditentukan warnanya melalui data yang tersimpan pada *array* yang bersangkutan.

Suatu citra biner (hitam-putih) menyediakan 2 bit data pada *array* tersebut. Data tersebut berupa representasi 1 untuk hitam dan 0 untuk putih, atau sebaliknya. Citra *grayscale* (abu-abu) menyediakan 8 bit pada *array* tersebut sebagai representasi dari kedalaman hitam-putih yang ditampilkan pada citra asli. Jumlah bit tersebut menghasilkan 256 kedalaman warna abu-abu pada citra *grayscale*.

Di sisi lain, sebuah citra warna asli (*true color*) menyediakan 24 bit untuk setiap sel *array* yang merepresentasikan besaran kombinasi warna R-G-B. Kombinasi tersebut dipecah menjadi tiga bagian sebesar masing-masing 8 bit untuk menghasilkan kedalaman masing-masing warna R (merah), G (hijau), dan B (biru). Ketiga aspek warna tersebut mengacu pada konsep fisik mengenai warna dasar spektrum cahaya.

Dapat dilihat pada perbandingan tersebut bahwa semakin kaya warna sebuah citra digital, maka semakin besar ukuran *file*-nya. Hal tersebut dapat memungkinkan suatu penyisipan data-data yang akan dikirim sebagai *embedded message*.

Teknik paling sederhana yang dipergunakan dalam steganografi citra digital adalah penyisipan nilai bit data pada representasi bit paling akhir pada data. Cara ini dikenal sebagai *least significant bit*. Dasar pertimbangan metode ini ialah bahwa representasi dari data pada citra digital *true color* adalah 24 bit untuk tiap pixel dengan 8 bit untuk tiap elemen warna dasar pada pixel tersebut. Dari 8 bit tersebut, nilai bit yang *least significant* akan memberikan perubahan warna yang tidak terlalu tampak pada penglihatan normal manusia. Hal tersebut menunjukkan bahwa sebuah pixel dalam citra digital *true color* (selain JPEG) menyediakan minimal tiga digit bit yang dapat ditempatkan untuk menyisipkan suatu citra *embedded.*

Teknik lainnya yang dilakukan adalah *Spread spectrum.* Teknik ini menghasilkan suatu *stego-object* berupa gambar *cover* yang di dalamnya mengandung sebaran *embedded message*. Teknik ini mengandalkan algoritma enkripsi-dekripsi tertentu lebih dari sekedar penyisipan bit pada posisi LSB. Melalui metode ini, boleh jadi pihak *eavesdropper* mampu mengekstraksi sebaran *embedded message,* terlebih lagi karena sifat sebarannya pun relatif kentara. Akan tetapi, informasi yang terekstraksi tidak mungkin terbaca sebagai sebuah pesan apabila pihak yang menmiliki informasi tersebut tidak disertai pengetahuan mengenai kunci maupun algoritma dekripsinya.

III. EKSPERIMEN KOMBINASI PENGAMANAN STEGANOGRAFI PADA KRIPTOGRAFI VISUAL

Sebagaimana diuraikan sebelumnya, dapat dinyatakan bahwa kriptografi visual menghasilkan minimal dua buah transparansi yang ketika ditumpukkan akan menghasilkan citra plainteks yang dapat diafirmasi secara visual. Akan tetapi, kemudahan yang dicapai tersebut mengakibatkan

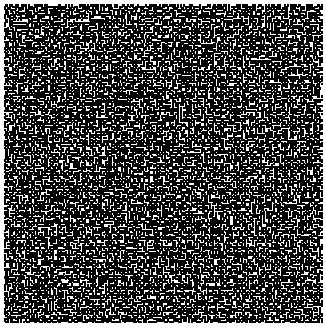
transmisi pesan yang dienkripsi menggunakan kriptografi visual membutuhkan minimal dua jalur atau dua aksi transmisi yang berbeda.

Berdasarkan hal tersebut, maka penulis merumuskan suatu penyelesaian dengan membangun suatu pengamanan citra digital menggunakan kriptografi visual yang diperkuat dengan aspek steganografi. Secara sederhana, metode tersebut dapat diurai sebagai berikut:

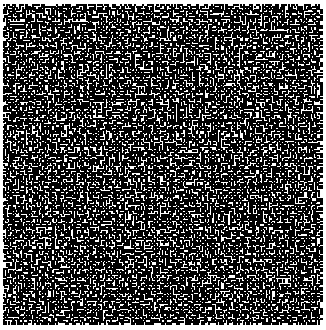
1. Citra plainteks dipecah menjadi sejumlah *n* transparansi melalui skema (n,n).
2. Steganografi terhadap transparansi-transparansi yang dihasilkan dilakukan terhadap satu citra digital dengan ukuran tertentu.

Eksperimen ini memanfaatkan perangkat steganografi yang dirancang oleh Lazarus Poli (IF '93) bernama DATAHide. Perangkat ini menyembunyikan citra digital dalam citra digital lainnya dengan menerapkan metode *least significant bit.* Sebagai sampel, akan digunakan citra-citra transparansi yang umum tersedia di internet.

Sampel yang digunakan pada eksperimen adalah citra-citra transparansi bitmap sebagai berikut, transparansi-transparansi tersebut adalah citra yang sama dengan objek yang ditampilkan di awal pembahasan:



Transparansi 1



Transparansi 2

Penerapan aspek steganografi tidak mungkin dilakukan antara kedua transparansi tersebut. Tidak ada citra transparansi yang dapat disembunyikan secara langsung terhadap transparansinya menggunakan metode *least significant bit*.

Pendekatan lainnya adalah dengan menggunakan citra tambahan sebagai *cover* tempat objek-objek yang hendak disembunyikan akan disisipkan.

Citra Cover

Sebagai awalan, percobaan dilakukan dengan memberlakukan steganografi antara gambar transparansi 1 dan 2 dengan citra cover. Penyisipan bit dilakukan secara satu-persatu. Transparansi 1 terlebih dahulu disisipkan pada cover, dan hasil sisipannya disisipi pula dengan Transparansi 2. Kedua transparansi dikunci penyisipannya dengan kunci yang berbeda.

Citra cover tidak berubah banyak. Akan tetapi, setelah dilakukan penyisipan kedua kalinya, sampel pertama tidak lagi dapat diekstraksi dengan baik. *Stego-object* yang dihasilkan hanya mampu

diekstraksi sampel yang paling akhir disisipkan padanya.

IV. ANALISIS

Aspek steganografi yang diterapkan pada eksperimen ini berdasar pada konsep penyisipan *least significant bit.* Sebagaimana dijelaskan di awal, metode penyisipan ini mengubah minimal 3 bit untuk tiap pixel gambar menjadi representasi bit gambar sisipan. Banyaknya alokasi yang disediakan bergantung pada pemrogram dan didasari pada perubahan warna yang terjadi melalui pengubahan nilai bit akibat penyisipan.

Oleh karena hal tersebut, maka penyisipan melalui pendekatan ini membutuhkan *cover-object* yang berukuran jauh lebih besar daripada objek yang disembunyikan. Penyembunyian objek dengan ukuran melebihi kapasitas akan membuat pola warna pixel *cover-object* terganggu sehingga ketertutupan objek sisipan tidak lagi terjamin.

Di sisi lain, dapat dilihat bahwa suatu citra *stego-object* hanya dapat disisipi satu citra lain. Penyisipan objek berikutnya akan merusak pola bit objek sisipan pertama. Demikian pula seterusnya sehingga pada akhirnya, hanya objek sisipan terakhir yang dapat diekstraksi dari suatu citra *stego-object.*

Berdasarkan dua analisis tersebut, maka kombinasi kriptografi visual dengan aspek steganografi yang dipaparkan penulis pada pembahasan sebelumnya bukanlah konsep yang dapat diimplementasikan dengan baik apabila sintesa solusi dilakukan melalui pendekatan dan teori yang telah dipaparkan. Hal inilah yang mendasari perkembangan sinergisasi kriptografi visual dan steganografi menggunakan pendekatan *multicover*, yaitu penyisipan setiap transparansi pada tepat satu *cover-object*.

V. KESIMPULAN DAN SARAN

Pendekatan kriptografi visual sederhana mampu menghasilkan cipherteks yang aman dengan aspek ketersampaian pesan yang relatif sederhana. Akan tetapi, distribusi cipherteks (transparansi) yang dilakukan secara terpisah merupakan suatu kelemahan dalam aspek efisiensi waktu. Selain itu, bentuk transparansi yang terkesan acak pun memancing kecurigaan pihak-pihak penyadap untuk menyatakan bahwa transparansi tersebut adalah suatu pesan tersembunyi. Oleh karenanya, dibutuhkanlah suatu aspek keamanan yang difasilitasi melalui steganografi.

Kombinasi kriptografi visual dengan aspek steganografi pada saat ini menggunakan pendekatan *multicover.* Hal tersebut merupakan suatu solusi yang dinilai paling layak diterapkan apabila menimbang hasil eksperimen dan analisis yang telah dilakukan penulis.

Adapun mengenai pendekatan kriptografi visual lainnya maupun metode steganografi yang belum terbahas, kedua hal tersebut tidak menutup kemungkinan adanya suatu metode penyembunyian citra digital yang memanfatkan kriptografi visual dan aspek steganografi. Hal tersebut dapat dijadikan bahan pertimbangan untuk pengembangan ide ini di masa mendatang.

REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Institut Teknologi Bandung, 2006.
[2] Naor, Moni dan Adi Shamir, *Visual Cryptography*, Eurocrypt 1994: 1-12.
[3] http://www.cs.fsu.edu/~yasinsac/group/slides/burke2.pdf
[4] http://www.jjtc.com/Steganography/
[5] http://www.petitcolas.net/fabien/steganography/

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, 16 Mei 2010

Anggrahita Bayu Sasmita
13507021