Pemanfaatan Steganografi dalam Kriptografi Visual

Muhamad Pramana Baharsyah

Laboratorium Ilmu dan Rekayasa Komputasi
Departemen Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung

Email: if13052@students.if.itb.ac.id

Abstraksi

Kriptografi visual yaitu sebuah teknik kriptografi data berupa gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Setiap bagian gambar tersebut adalah subset dari gambar awalnya. Jika dihasilkan n bagian dalam proses enkripsi, maka jika hanya terdapat n – 1 bagian, gambar tidak dapat didekripsi. Tujuan awal penggunaan metode ini yaitu untuk membuat sebuah model kriptografi data berupa gambar atau citra yang dapat didekripsi tanpa bantuan komputer.

Steganografi ialah ilmu atau seni penyembunyian sebuah pesan rahasia di dalam pesan lainnya. Steganografi digunakan untuk menyampaikan pesan tanpa menimbulkan kecurigaan bahwa pesan yang dikirim merupakan sebuah pesan rahasia. Steganografi memiliki kelemahan yaitu jika seseorang mengetahui bahwa dalam objek tersebut terdapat pesan rahasia, maka ia dapat mencoba mengekstraksi pesan tersebut. Untuk mengatasi kelemahan tersebut maka metode steganografi dan kriptografi visual digabungkan menjadi sebuah metode baru untuk menjaga kerahasiaan pesan berupa gambar.

***Kata kunci**:* Kriptografi visual, Steganografi

1. Pendahuluan

Komunikasi data melalui jaringan komputer memiliki berbagai keuntungan dan memberikan banyak kemudahan. Salah satu keuntungan yang didapatkan yaitu waktu yang diperlukan untuk menyampaikan pesan dari suatu tempat ke tempat lainnya dapat dihemat. Keuntungan lainnya ialah biaya pengiriman yang kecil. Namun di antara sekian banyak keuntungan tersebut terdapat sebuah kelemahan yang dirasakan berdampak besar pada pengiriman pesan melalui jaringan komputer. Kelemahan tersebut berasal dari masalah keamanan jaringan komputer itu sendiri.

Pengiriman pesan melalui jaringan komputer memiliki beberapa kelemahan dari sisi keamanan[TAN03], antara lain :

1) Kerahasiaan pesan
2) Keotentikan pesan
3) Keotentikan pengirim pesan, dan
4) Integritas pesan

Pada umumnya masalah keamanan tersebut diakibatkan adanya sejumlah orang yang berusaha mendapatkan keuntungan dengan cara yang curang, orang yang ingin menyerang orang lainnya secara sembunyi–sembunyi ataupun terang–terangan, atau malah hanya agar mendapatkan perhatian [TAN03].

Kriptografi menjadi salah satu alternatif dalam meningkatkan keamanan pengiriman pesan dalam saluran komunikasi yang berupa jaringan komputer tersebut. Pesan yang akan dikirim terlebih dahulu dienkripsi sebelum masuk ke saluran komunikasi tersebut. Tujuan dari pengenkripsian pesan ialah agar pesan hanya dapat dibaca oleh orang yang memang berhak membaca pesan yang dikirimkan itu. Akan tetapi, pesan yang dienkripsi tetap dapat dibaca oleh orang yang tidak berhak membacanya melalui berbagai cara antara lain :

1) *Brute force attack*
2) *Analytical attack*

Steganografi merupakan cara lain yang cukup efektif untuk meningkatkan keamanan komunikasi dalam saluran informasi yang tidak aman. Steganografi menyembunyikan keberadaan sebuah pesan di dalam suatu objek. Dengan menggunakan metode ini, pesan rahasia dapat disampaikan ke tujuan melalui saluran komunikasi yang tingkat keamanannya rendah tanpa menimbulkan kecurigaan bahwa di dalam objek tersebut terdapat sebuah pesan rahasia. Namun jika ada pihak ketiga yang berhasil menyusup ke dalam jaringan komunikasi tersebut dan menyadari keberadaan pesan rahasia pada objek yang ditransmisikan melalui jaringan komunikasi itu, ia dapat mencoba memecahkan pesan yang terdapat dalam gambar tersebut. Pada prakteknya, pihak ketiga tersebut tidak akan dapat dengan mudah mendapatkan pesan yang tersembunyi itu. Diperlukan usaha untuk mendapatkan pesan tersebut, namun pada akhirnya pesan itu pasti berhasil didapatkan.

Sebuah solusi yang telah diterapkan secara umum terhadap permasalahan tersebut ialah dengan melakukan enkripsi terhadap pesan yang disisipkan pada objek sebelum objek ditransmisikan melalui saluran komunikasi. Solusi ini bisa jadi membingungkan pihak ketiga yang berhasil mendapatkan objek yang berisi pesan rahasia tersebut untuk sementara waktu. Namun sekali lagi solusi yang ditawarkan ini juga dirasa masih kurang aman. Setelah pihak ketiga berhasil mengetahui algoritma yang digunakan untuk mengenkripsi pesan maka ia dapat melakukan kriptanalisis terhadap pesan tersebut.

Pertukaran pesan rahasia tidak hanya dilakukan antara individu dengan individu lainnya. Terkadang, seorang ingin mengirimkan pesan rahasia kepada sekelompok orang. Hanya saja ia tidak yakin jika pesan yang ia kirimkan diterima oleh seluruh anggota kelompok tersebut. Jika masalah keamanan pada pertukaran pesan antar individu saja sudah merupakan masalah yang kompleks, maka pada kasus ini dibutuhkan tingkat keamanan yang jauh lebih tinggi agar tujuannya tercapai.

Untuk mengatasi masalah tersebut, diajukan sebuah metode baru untuk meningkatkan keamanan pengiriman pesan pada saluran komunikasi yang rentan terhadap serangan. Metode yang diajukan ialah dengan memodifikasi teknik kriptografi visual (*visual cryptography*) yang dikombinasikan dengan steganografi.

2. Pengenalan Kriptografi Visual

Kriptografi Visual ialah sebuah teknik kriptografi di mana sebuah data berupa gambar atau citra dienkripsi, dengan suatu cara, menjadi sejumlah gambar, sehingga dapat didekripsi hanya dengan indera penglihatan manusia, tanpa bantuan komputer, jika seluruh bagian gambar ditumpuk bersamaan[NAO95].

Kriptografi visual, pertama kali diajukan oleh Moni Naor dan Adi Shamir, ialah sebuah teknik kriptografi baru di mana cipherteks dapat didekripsi oleh alat penglihatan manusia. Akibatnya, tidak dibutuhkan komputasi kriptografi yang rumit untuk proses dekripsinya. Ide awalnya ialah dengan membagi sebuah gambar menjadi dua bagian, sedemikian sehingga satu gambar menjadi cipherteks dan gambar lainnya menjadi kunci. Kedua gambar ini lalu dapat dikirim secara terpisah kepada tujuan. Setibanya di tujuan, dilakukan dekripsi dengan cara mencetak kedua gambar tersebut pada lembar transparan. Kedua lembar tersebut lalu dibentuk menjadi sebuah tumpukan sehingga gambar asli dapat terlihat dengan mata. Dengan demikian proses mendapatkan plainteks(gambar 1) dapat dilakukan oleh siapa saja yang memiliki cipherteks (gambar 2) dan kunci (gambar 3) secara bersamaan.

Contoh kriptografi visual :

Gambar 1 : Plain Text

Gambar 2 : Cipher Text

Gambar 3 : Kunci

Cara Kerja Kriptografi Visual

Untuk memudahkan pemahaman mengenai kriptografi visual, gambar 4 menampilkan proses sederhana dari kriptografi visual. Pada gambar tersebut, (a) adalah gambar yang ingin dikirim, sebelum dikirim, gambar terlebih dahulu dienkripsi dengan teknik kriptografi visual menjadi dua buah gambar, (b) dan (c). Lalu masing-masing gambar dikirim ke tujuan secara terpisah. Setelah sampai di tujuan, penerima mencetak gambar (b) dan (c) secara terpisah, masing-masing pada satu lembar transparan. Kemudian untuk melihat gambar aslinya penerima menumpuk kedua lembar tersebut sehingga didapatkan gambar (d).

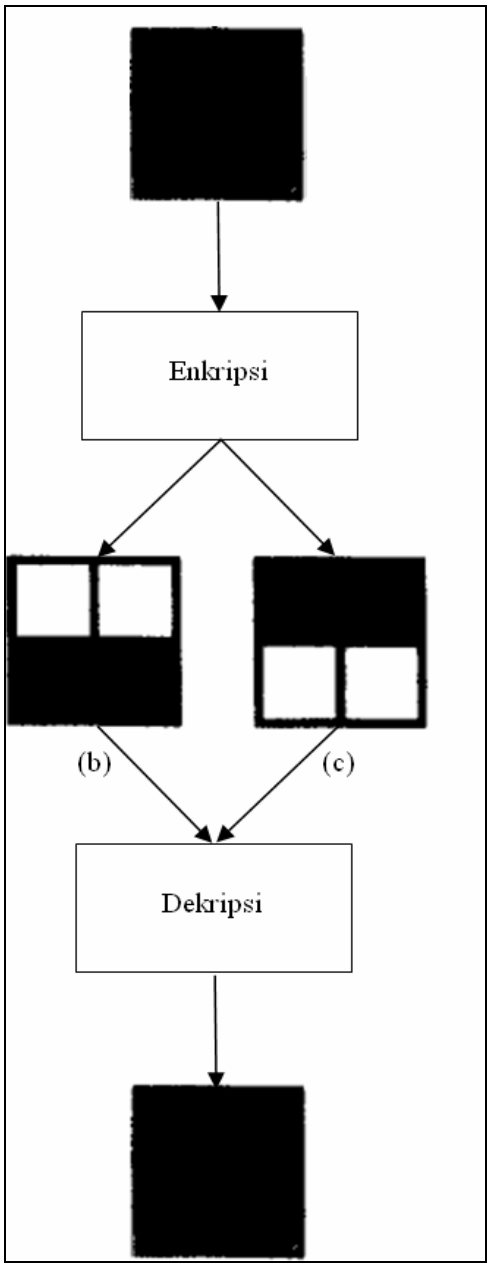
Pada contoh tersebut dapat disimpulkan jika seorang memiliki kedua bagian dari dua buah gambar hasil enkripsi, maka ia akan dapat mendekripsi gambar tersebut. Skema ini dinamakan skema "n dari n". Skema n dari n merupakan skema teknik kriptografi visual di mana dihasilkan n buah gambar atau objek pada proses enkripsi lalu untuk mendekripsinya dibutuhkan juga n buah objek hasil enkripsi.

Selain skema n dari n, terdapat pula skema lain yaitu k dari n ($k < n$). Pada skema ini hanya dibutuhkan sejumlah k objek hasil enkripsi untuk mendapatkan objek asal. Jika jumlah objek kurang dari k maka hasil dekripsi akan berbeda dengan objek asalnya. perlu diperhatikan juga jika objek yang dimiliki lebih dari k, maka objek asli tetap dapat didapatkan melalui proses dekripsi yang sama dengan proses dekripsi dengan menggunakan skema n dari n. Contoh skema ini dapat dilihat pada Gambar 5.

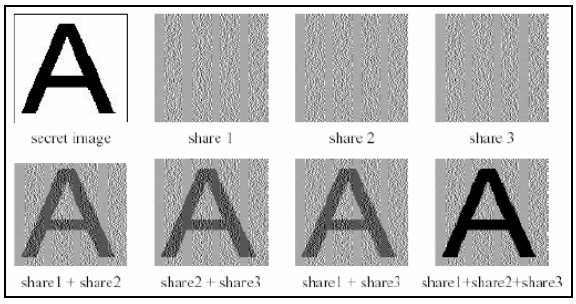
Model Kriptografi Visual

Model yang paling sederhana dari permasalahan visual kriptografi ialah dengan menggunakan gambar yang hanya terdiri dari sejumlah pixel berwarna hitam atau putih saja. Setiap pixel ditangani secara terpisah[i] [NAO95]. Tiap – tiap pixel akan muncul pada n objek hasil enkripsi (*share*). Tiap *share* adalah subset dari objek asli. Pemodelan sederhana ini dapat ditampilkan dalam representasi matriks boolean yang berukuran m x n di mana m ialah lebar gambar dan n adalah tingginya dalam satuan pixel. Jika suatu pixel berwarna hitam pada gambar aslinya, maka pada matriks digambarkan dengan nilai 1 atau true, sebaliknya jika pixel berwarna putih maka digambarkan dengan nilai 0 atau false. Gambar 6 menampilkan matriks untuk gambar yang berwarna hitam seluruhnya dan berukuran 6 x 6.

Jika gambar tersebut dienkripsi dengan metode yang paling sederhana dari kriptografi di atas dengan jumlah *share* = 2, maka salah satu kemungkinan dua buah gambar yang dihasilkan ialah seperti gambar 7.



Gambar 4 : Cara kerja Kriptografi Visual



Gambar 5 : Contoh Penggunaan Skema k dari n (k = 2, n = 3)

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Gambar 6 : Model Untuk Gambar Berukuran 6 x 6 Berwarna Hitam

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Gambar 7 : Hasil Enkripsi Gambar 5

3. Pengembangan Kriptografi Visual

Metode awal tersebut sangat sederhana dan memiliki tingkat keamanan yang kurang baik. Shamir dan Naor pada papernya mengajukan cara lain untuk memodelkan masalah ini. Dengan metode ini, tiap pixel tidak direpresentasikan dalam sebuah elemen matriks, melainkan dalam m elemen matriks. Maksudnya, setiap pixel dibagi menjadi m buah subpixel, misalnya pada gambar 8, m = 4, yang jika digabungkan masih dapat diterima oleh persepsi manusia sebagai satu warna, hitam atau putih. Misal, suatu pixel berwarna hitam, dengan m = 4, dapat direpresentasikan dalam sebuah matriks 2 x 2 sebagai berikut :

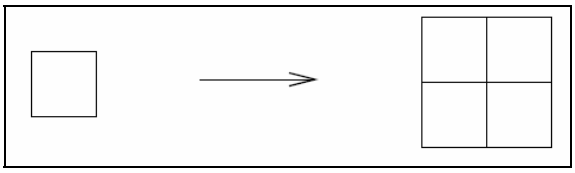
$$\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}$$

atau

$$\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}$$

atau

$$\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$$



Gambar 8 : Pembentukan subpixel dengan m = 4

Nilai yang dihasilkan dari transformasi matriks tersebut menjadi pixel kembali akan mengalami *noise*. Maksudnya, pada contoh di atas sebuah pixel yang berwarna hitam, setelah ditransformasikan akan berwarna keabu-abuan. Untuk menginterpretasikan sebuah pixel yang memiliki level keabu-abuan tersebut menjadi warna hitam atau putih, indera penglihatan manusia akan dengan mudah melakukannya. Sedangkan untuk pemodelannya di komputer diperlukan sebuah formula untuk menentukan ambang batas antara hitam dan putih.

Hamming Weight digunakan untuk memberi batasan antara hitam dan putih pada pixel yang memiliki tingkat keabu-abuan. Hamming Weight dari suatu pixel dilambangkan dengan H(V). Tabel berikut menggambarkan hubungan antara H(V) dengan warna yang direpresentasikannya :

Warna	H(V)
Hitam	$H(V) \geq d$
Putih	$H(V) < d - \alpha m$

Di mana :
H(V) : Hamming Weight
d : ambang batas ($1 \leq d \leq m$)
α : kontras
m : jumlah subpixel

Hasil transformasi suatu gambar berupa sebuah matriks boolean S yang berukuran n x m. S_{ij} bernilai 1 jika dan hanya jika subpixel ke-j pada share ke-i berwarna hitam. Level keabu-abuan didapatkan dengan menumpuk tiap share. Lalu diinterpretasikan sebagai hitam atau putih sesuai dengan Hamming Weight-nya.

Efek warna hitam yang diakibatkan suatu subpixel pada suatu lembar tidak dapat dinegasikan oleh suatu subpixel dari lembar lainnya. Akibatnya pada proses enkripsi akan muncul *noise* dan *noise* tersebut tidak dapat dihilangkan pada proses dekripsi.

Proses tersebut di atas berlaku untuk skema n dari n. Sedangkan untuk skema k dari n dilakukan teknik yang hampir mirip. Solusi untuk skema k dari m terdiri dari dua buah koleksi matriks boolean berukuran n x m, C_0 dan C_1. Untuk membagi pixel berwarna putih, dipilih salah satu dari matriks pada C_0, sedangkan untuk membagi warna hitam, dipilih salah satu matriks dari C_1. Matriks yang terpilih merupakan representasi dari m subpixel pada masing-masing n lembar transparan. Solusi dianggap valid jika seluruh kondisi berikut terpenuhi:

1) Untuk sembarang matriks M pada C_0, hasil operasi OR dengan V dengan sembarang baris k dari n memenuhi $H(V) < d - \alpha m$.

2) Untuk sembarang matriks M pada C_1, hasil operasi OR dengan V dengan sembarang baris k dari n memenuhi $H(V) \geq d$.

3) Untuk sembarang j < k baris yang dipilih, submatriksnya muncul dengan frekuensi yang sama pada C_0 dan C_1.

Kondisi ketiga mengimplikasikan kesulitan yang akan dialami oleh kriptanalis untuk menentukan apakah pixel pada share tersebut berwarna hitam atau putih. Ada tiga parameter yang mempengaruhi kualitas kriptografi visual :

1) m, jumlah pixel dalam share, semakin besar nilai m, semakin besar jumlah noise yang ditimbulkan, sehingga nilai m diusahakan sekecil mungkin.

2) α, perbedaan relatif antara share yang sudah digabung dari pixel berwarna putih dengan hitam. Semakin besar nilainya akan semakin baik.

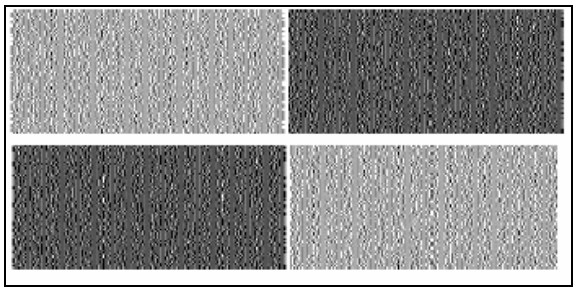
3) r, ukuran C_0 dan C_1. Nilai r untuk C_0 dan C_1 tidak harus sama. Nilai log r merepresentasikan jumlah bit acak yang diperlukan untuk menciptakan share tanpa mengalami penurunan kualitas gambar

4. Kriptografi Visual dan Steganografi

Ide yang dilontarkan Naor dan Shamir tersebut memicu riset di bidang kriptografi khususnya pada kriptografi visual. Beberapa tahun setelah Naor dan Shamir memublikasikan ide mereka, tepatnya pada tahun 1997, E. Verheul dan H. V. Tilborg berhasil menerapkan kriptografi visual pada gambar dan citra berwarna. Hanya saja metode yang diusulkan oleh mereka memiliki beberapa kekurangan antara lain hasil penggabungan kembali yang memiliki noise yang tinggi. Selain itu, share yang dihasilkan tidak memiliki makna.

Share yang tidak memiliki makna akan dengan mudah menimbulkan kecurigaan bahwa gambar tersebut adalah gambar yang mengandung pesan rahasia. Pesan rahasia yang terdapat di dalam gambar tersebut bisa berupa hasil dari enkripsi ataupun objek tersebut adalah media dari steganografi. Sebagai contoh, gambar 9 adalah gambar asli dan gambar 10 adalah hasil enkripsinya menggunakan kriptografi visual

Gambar 9 : Gambar Asli, sebelum dienkripsi



Gambar 10 : Setelah dienkripsi menjadi 4 buah share yang tidak bermakna

Dari gambar tersebut terlihat bahwa masing-masing share tidak bermakna dan akan dengan mudah diketahui bahwa gambar tersebut mengandung pesan tersembunyi.

Untuk mengatasi masalah tersebut maka digunakan metode steganografi sebagai pelengkap metode kriptografi visual. Bagaimana cara kerja metode ini akan dibahas kemudian.

Steganografi

Steganografi ialah teknik penyembunyian pesan rahasia ke dalam sebuah media sehingga tidak menimbulkan kecurigaan akan keberadaan pesan rahasia tersebut.

Terdapat dua istilah penting dalam steganografi yaitu pesan yang akan disampaikan (objek) dan wadah penampung pesan tersebut (media).

Pada awalnya steganografi diimplementasikan dengan berbagai metode klasik seperti menyembunyikan tulisan di kulit kepala. Selain itu steganografi juga bisa dilakukan dengan mengganti tiap karakter dari pesan yang akan disampaikan menjadi sebuah kata di mana karakter pertama tiap kata tersebut adalah karakter dari pesan yang akan disampaikan.

Seiring munculnya komputer sebagai alat pengelola data digital, steganografi juga berkembang menjadi steganografi digital. Selanjutnya kata steganografi yang ditulis pada makalah ini akan merujuk pada steganografi digital.

Steganografi digital menyembunyikan pesan digital pada media digital seperti file gambar, file suara ataupun file video. Penyisipan pesan ke dalam media digital akan mengurangi kualitas media tersebut. Oleh karena itu dalam melakukan steganografi perlu dipertimbangkan :

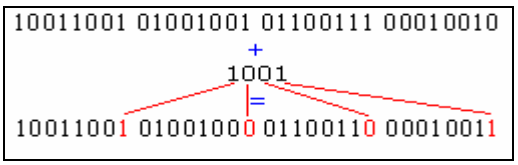
1) Kualitas media steganografi tidak jauh berubah.
2) Ketahanan pesan jika terjadi perubahan pada media.
3) Pesan yang disembunyikan dapat diekstraksi tanpa mengalami kehilangan informasi.

Teknik Penyembunyian Pesan

Teknik yang paling sederhana untuk menyembunyikan pesan dalam sebuah media digital ialah dengan mengubah satu bit dari media dengan bit dari pesan. Biasanya bit terakhir dari suatu byte diganti dengan bit dari pesan.

Misalkan pesan yang ingin disampaikan panjangnya 4 bit yaitu 1001. Media steganografi terdiri atas 4 byte, 10011001 01001001 01100111

00010010. Maka dengan teknik ini dihasilkan media yang telah disisipkan pesan rahasia sebagai berikut 10011001 01001000 01100110 00010011.



Gambar 11 : Contoh Steganografi

Teknik seperti itu disebut juga teknik LSB (Least Significant Bit). Dengan mengganti bit terkanan dari bit berarti hanya mengubah nilai byte secara keseluruhan dengan satu nilai, akibatnya perubahan pada media tidak akan dapat ditangkap oleh indera manusia.

Karena pada metode LSB tiap bit pesan hanya dapat disisipkan pada satu byte media, maka ukuran pesan yang dapat disembunyikan jauh lebih kecil daripada ukuran media penyembunyian pesan. Dalam hal ini ukuran pesan maksimal yang dapat ditampung ialah $^{1}/_{8}$ ukuran media.

Terdapat beberapa teknik steganografi lainnya yang mampu menyembunyikan pesan dalam media digital. Namun, pada makalah ini hanya disampaikan salah satu saja karena yang perlu diperhatikan ialah bagaimana cara kerja steganografi itu sendiri secara umum.

5. Pemanfaatan Steganografi dalam Kriptografi Visual

Riset dalam bidang kriptografi visual sangat ekstensif dilakukan setelah dipublikasikannya makalah yang disusun oleh Naor dan Shamir pada tahun 1995. Algoritma kriptografi visual yang baru hasil modifikasi atau penyempurnaan algoritma sebelumnya bermunculan.

Kegunaan kriptografi visual yang tadinya hanya untuk mengenkripsi pesan agar tidak perlu didekripsi menggunakan komputasi mulai ditinggalkan. Kriptografi visual juga digunakan untuk mengatasi permasalahan "6 perampok".

Masalah 6 perampok ialah masalah pembagian rahasia bersama (secret sharing). Terdapat 6 orang perampok yang memiliki sebuah rekening bank. Permasalahannya ialah mereka tidak percaya satu sama lain, namun mereka berasumsi bahwa tidak mungkin 3 orang atau lebih berkolusi untuk mengkhianati yang lainnya. Oleh karena itu para perampok, dengan suatu cara, membagi kata kunci rekening tersebut menjadi 6 bagian di mana dibutuhkan 3 atau lebih perampok untuk merangkai kata kunci.

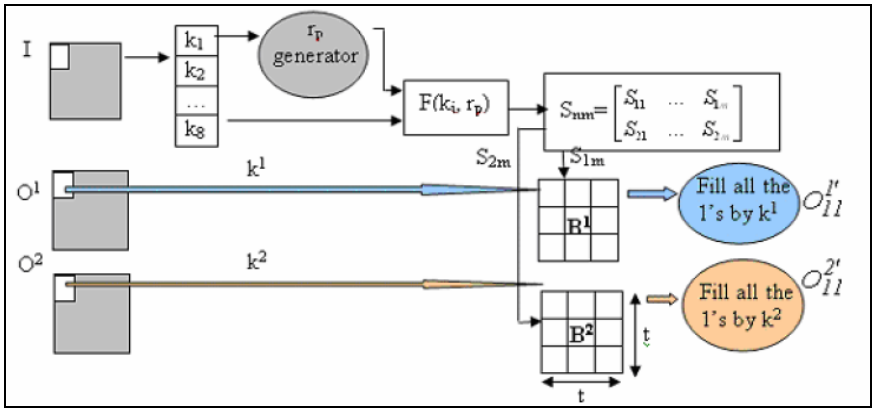
Selain permasalahan 6 perampok, kriptografi visual juga dapat digunakan untuk mengenkripsi pesan gambar tanpa menimbulkan kecurigaan orang lain yang tidak berhak melihat gambar tersebut.

C. Chang, C. Tsai, dan T. Chen, pada Juli 2000 mengajukan kriptografi visual baru yang tidak memerlukan penumpukan share untuk menghasilkan objek asli. Teknik ini memanfaatkan gambar lain(cover) untuk menyimpan tiap share. Teknik inilah yang lebih mudah digunakan dalam aplikasi kriptografi visual. Akan tetapi, teknik ini membutuhkan media penyimpanan tambahan untuk menyimpan Color Index Table (CIT) agar noise pada gambar hasil dekripsi tidak terlalu besar. waktu eksekusi juga bertambah karena dibutuhkan operasi untuk memeriksa tabel tersebut.

Chang, C. C. dan Yu. T. X. mengajukan teknik yang lebih baik dalam menerapkan kriptografi visual pada gambar berwarna. Teknik yang diajukan ini tidak membutuhkan CIT. Tidak terdapat noise pada objek hasil dekripsi menggunakan teknik ini. Namun tiap share yang dihasilkan(camouflage) memiliki noise yang cukup besar. Contoh penggunaan teknik ini dapat dilihat pada gambar 7.

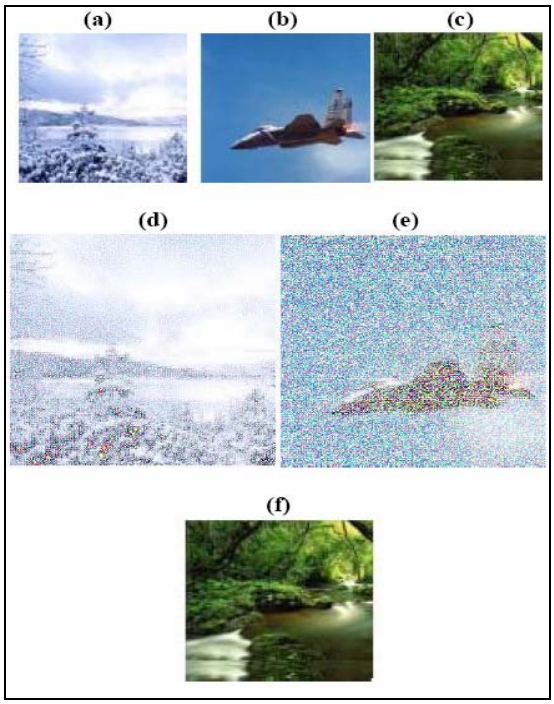
Pada gambar 13 (a) adalah cover 1, (b) adalah cover 2, (c) adalah objek gambar yang akan disembunyikan, (d) camouflage 1, (e) camouflage 2, dan (f) adalah hasil dekripsi.

Teknik ini menggunakan sejumlah objek gambar lainnya untuk menyimpan share yang dihasilkan. Objek gambar yang digunakan untuk menyimpan share yang dihasilkan dalam proses enkripsi disebut cover object. Sedangkan cover object yang telah disisipkan share disebut camouflage.



Gambar 12 : Enkripsi Menggunakan Metode Kriptografi Visual Chang dkk.

Dengan menggunakan teknik ini, objek hasil dekripsi tidak akan mengalami noise. Akan tetapi camouflage yang dihasilkan setelah menyisipkan share memiliki tingkat noise yang tinggi.



Gambar 13 : Kriptografi Visual Chang dkk.

Deskripsi Metode

Misalkan gambar yang ingin dienkripsi ialah sebuah gambar dengan 256 warna. Setiap warna direpresentasikan dalam bentuk array 8-bit. Prinsip utamanya ialah dengan membagi tiap pixel menjadi sejumlah m subpixel dan melekatkannya pada n buah share. perbedaannya dengan metode sebelumnya ialah pada metode ini tidak digunakan operasi OR melainkan digunakan operasi XOR pada proses dekripsinya.

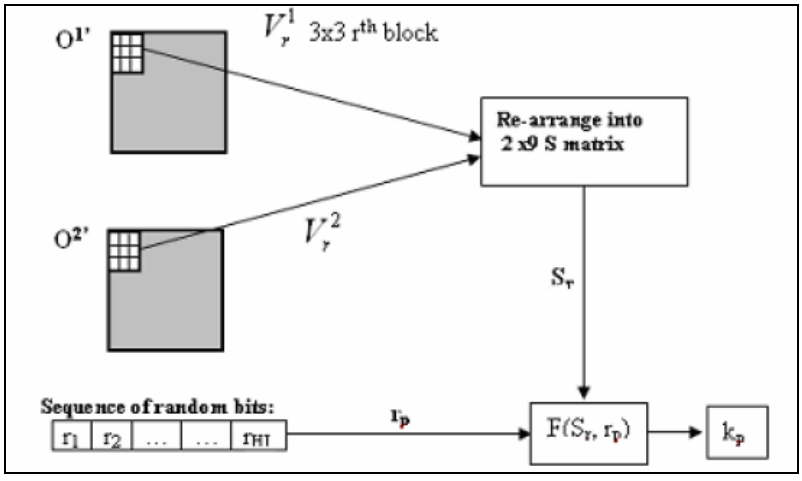
Langkah – langkah yang dilakukan untuk menghasilkan camouflage ialah sebagai berikut :

1) Pilih n buah cover object yang memiliki ukuran sama dengan objek yang akan dienkripsi.
2) Buat array of bits untuk setiap pixel pada objek yang akan dienkripsi.
3) pilih integer r, di mana $1 \leq r \leq m$. untuk masing – masing pixel.
4) bentuk S yang memenuhi persamaan $k_i = S_{1j} \oplus S_{2j}$

   where $k_i = S_{1j} \oplus S_{2j}$ and $j = \begin{cases} i & if\ i < r \\ i+1 & if\ i > r \end{cases}$
5) Sisipkan bit pada S ke cover object.

Gambar 12 menggambarkan proses pengenkripsian satu pixel pada gambar asli.

Untuk menghasilkan objek asli, diperlukan camouflage beserta array bits yang diciptakan pada proses enkripsi. proses dekripsinya sendiri dapat digambarkan seperti gambar 14

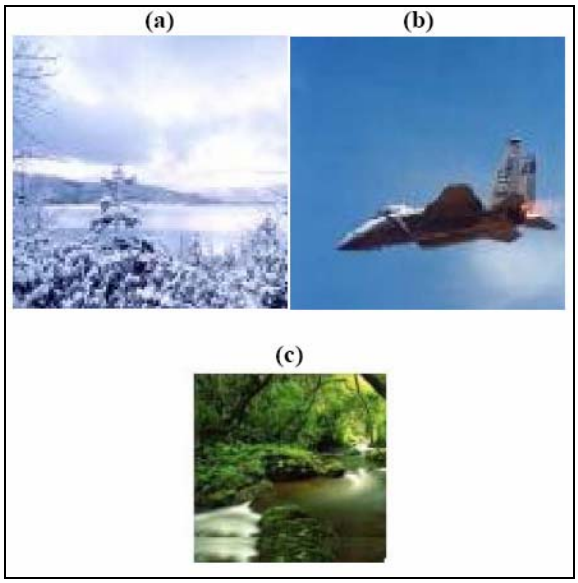


Gambar 14 : Dekripsi Menggunakan Metode Kriptografi Visual Chang dkk.

R.Youmaran, A. Adler dan A. Miri mengusulkan sebuah pendekatan baru hasil pengembangan metode Chang dkk. Modifikasi yang dilakukan ialah sebelum membangkitkan subpixel, tiap pixel ditambah 1, hal tersebut dilakukan untuk menjamin tidak ada pixel yang bernilai 0. Akan tetapi nilai pixel maksimum dibatasi 255.

Hasil yang diperoleh melalui algoritma ini jauh lebih baik daripada metode sebelumnya. Gambar 10 menunjukkan perbedaan kualitas antara metode ini dengan metode Chang dkk.

Gambar 15 (a) adalah cover object 1, (b) adalah cover object 2, dan (c) adalah gambar hasil dekripsi.



Gambar 15 : Kriptografi Visual Youmaran dkk.

6. Kesimpulan

Naor dan Shamir berhasil menciptakan suatu metode pengenkripsian pesan berupa gambar yang baru yang dinamakan kriptografi visual

Kriptografi visual pada awalnya digunakan untuk melakukan enkripsi pada pesan berupa gambar agar proses pada dekripsinya tidak diperlukan adanya bantuan komputer. Pada perkembangannya, kegunaan kriptografi visual juga turut berkembang.

Melalui bantuan steganografi, pesan rahasia dapat disampaikan tanpa menimbulkan kecurigaan pihak lain yang tidak berhak membaca isi pesan tersebut.

Penggunaan metode steganografi untuk kriptografi visual memberikan berbagai keuntungan antara lain :

1) Tingkat keamanan pesan gambar yang ingin disampaikan sangat baik.
2) Tidak timbul kecurigaan pada orang lain yang mendapatkan sebuah share dari kriptografi visual.
3) Pesan hanya dapat dibaca jika jumlah share cukup.

Namun, diantara kelebihan tersebut, kriptografi visual memiliki beberapa kendala seperti proses menghasilkan sejumlah share yang kompleks dan lama.

Peluang riset di bidang kriptografi visual masih terbuka karena algoritma-algoritma yang sudah ada masih memiliki berbagai kelemahan.

Daftar Pustaka

[MUN03] Munir, R. *Diktat Kuliah IF5054 Kriptografi Program Studi Teknik Informatika Institut Teknologi Bandung*(2006).

[NAO95] N.Naor and A. Shamir, *Visual Cryptography, Advances in Cryptology*: Eurocrypt '94, Springer - Verleg, Berlin, pp l-129 (1995).

[TAN95] Tanenbaum, A, *Computer Networks 4th edition*: Prentice Hall, New Jersey, (2003).

[YOU06] Youmaran, R, dkk. *An Improved Visual Cryptography Scheme for Secret Hiding*. paper (2003).

[i] Penanganan sejumlah pixel secara bersamaan akan memberikan hasil yang lebih baik. [NAO95]