Studi Kriptografi Visual dengan Enkripsi Gambar Lain

Franciscus Borgias Dian Paskalis - 13507048
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17048@students.if.itb.ac.id

***Abstract*—Kriptografi Visual adalah bentuk khusus dari enkripsi gambar yang diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994 di EUROCRYPT 1994. Teknik ini dapat membuat pesan atau gambar tersembunyi dalam minimal 2 gambar lain. Kriptografi Visual merupakan bentuk teknik kriptografi yang membuat manusia dapat melakukan dekripsi gambar tanpa bantuan komputer. Untuk penerimanya, teknik ini merupakan teknik paling sederhana tetapi juga merupakan sistem yang sangat aman. Teknik ini terbilang baru dan inti dari teknik ini adalah memisah suatu gambar menjadi *n* bagian.**

Kriptografi Visual dikatakan sebagai teknik enkripsi gambar yang terbaik dan sempurna. Suatu gambar utuh ketika dikenai teknik kriptografi visual dapat menjadi beberapa bagian berbeda yang tidak memiliki arti. Tiap bagian dari gambar-gambar tersebut ditampilkan dengan transparensi tertentu. Tetapi ketika gambar-gambar tersebut disatukan kembali, gambar akan menampilkan gambar awal (tidak tepat sama, tetapi garis besarnya terlihat) sebelum dikenai teknik ini.

Dalam Kriptografi Visual, digunakan minimal dua gambar yang memiliki transparansi : lapisan (*layer*) pertama berisi piksel acak, dan lapisan berikutnya berisi informasi rahasia. Kriptografi Visual bekerja dengan lapisan-lapisan yang memiliki piksel identik sama atau saling melengkapi, bentuk visual dari operasi XOR. Membaca informasi pada hasil enkripsi menggunakan teknik ini hanya mungkin ketika lapisan-lapisan tersebut diletakkan tepat di atas satu dengan lainnya. Jika piksel acak pada lapisan pertama tersebut dibangkitkan dengan benar-benar acak, hal ini dapat dilihat sebagai sistem *one-time pad*. Dalam kasus ini, memperoleh informasi rahasia dari salah satu lapisan gambar akan tidak mungkin dilakukan jika tidak memiliki lapisan-lapisan gambar lainnya, sehingga hal ini membuat Kriptografi Visual memiliki keamanan yang absolut.

Kriptografi Visual ini berbeda dari cara enkripsi lainnya yang digunakan untuk menyembunyikan pesan pada gambar. Pada umumnya enkripsi pesan yang menggunakan gambar lainnya dilakukan dengan cara menyimpan bit-bit pesan pada bit-bit terkecil pada suatu gambar sehingga gambar yang dijadikan *host* penyimpan pesan tidak akan berubah banyak. Pada teknik enkripsi tersebut hanya perlu mengambil tiap LSB (*Least Significant Byte*) dari gambar yang telah dienkripsi untuk memperoleh pesan rahasia yang terkandung dalamnya. Teknik ini dikenal dengan nama steganografi.. Sedangkan pada teknik enkripsi lainnya dibutuhkan gambar *host* asli sebelum dikenai enkripsi untuk dibandingkan dengan gambar hasil enkripsi sehingga pesan yang terkandung di dalamnya dapat diperoleh.

Dalam aplikasinya ternyata kriptografi visual dapat dikombinasikan dengan teknik pengolahan gambar yang lain untuk menambah kerumitan algoritma. Sampai sekarang teknik ini masih belum dapat dipecahkan.

***Index Terms*—kriptografi visual, penyembunyian pesan, pembagian rahasia, pemrosesan gambar**

I. PENDAHULUAN

Pada umumnya, penyembunyian informasi dengan menggunakan gambar dapat dilakukan dengan menyisipkan informasi pesan pada bit-bit terkecil (LSB, yaitu *Least Significant Byte*) data gambar yang digunakan. Hal ini dikenal secara umum dengan sebutan steganografi. Tentu saja bit-bit tersebut akan mengalami perubahan, tetapi karena bit-bit yang diubah adalah bit terkecil maka gambar secara keseluruhan tidak akan mengalami perubahan yang berarti. Teknik ini dinilai cukup aman karena gambar yang telah dienkripsi tidak akan menimbulkan penyusup yang berusaha mendapatkan pesan curiga. Tentu saja, untuk melakukan dekripsi diperlukan bantuan komputer untuk mengolahnya.

Teknik enkripsi lain dapat dilakukan dengan menyisipkan informasi rahasia pada gambar dengan menggunakan modifikasi teknik *watermarking*. Sayangnya juga, teknik ini sendiri memiliki kelemahan, yaitu penerima pesan harus memiliki gambar asli yang akan dibandingkan dengan gambar hasil enkripsi sehingga dapat diperoleh pesan di dalamnya. Pendistribusian gambar asli ini sendiri dapat diinterupsi oleh pihak lain sehingga teknik ini sendiri dapat jadi tidak aman.

Pada tahun 1994 di *EUROCRYPT'94*, Moni Naor dan Adi Shamir mengajukan pertanyaan yang memikat: apakah mungkin membuat skema pembagian rahasia yang membuat gambar dapat direkonstruksi secara visual dengan menggabungkan dua bagian gambar? Tiap bagian akan berisi transparensi yang terdiri dari piksel hitam dan putih. Pemeriksaan pada salah satu bagiannya harus tidak mengungkapkan informasi mengenai gambar.

Mereka mengembangkan suatu skema yang menggunakan minimal dua buah gambar dan gambar-gambar tersebut harus memiliki transparansi. Skema pembagian rahasia ini disebut Kriptografi Visual. Lapisan pertama berisi piksel acak, dan lapisan berikutnya berisi informasi rahasia. Kriptografi Visual

dapat dikatakan merupakan bentuk visual dari operasi XOR. Membaca informasi pada hasil enkripsi menggunakan teknik ini hanya mungkin ketika lapisan-lapisan tersebut diletakkan tepat di atas satu dengan lainnya.

Keamanan skema ini dianggap sangat tinggi dan sampai sekarang tidak dapat dipecahkan. Cara untuk mendekripsi pesan tersebut juga sangat mudah dan dapat dilakukan tanpa bantuan komputer, berbeda dengan teknik kriptografi lain yang membutuhkan bantuan komputer untuk dekripsinya. Untuk dekripsi Kriptografi Visual kita cukup mencetak gambar hasil enkripsi pada kertas-kertas putih tipis. Kemudian kertas tersebut cukup ditumpuk di atas satu sama lain dan diarahkan ke cahaya terang, gambar-gambar pesan tersebut akan saling bertumpukan dan kita dapat melihat pesan yang terkandung dalamnya. Keuntungan teknik ini juga adalah kita memerlukan bantuan visual secara manual (mata) untuk membaca pesan tersebut.

II. STEGANOGRAFI

Steganografi berasal dari bahasa Yunani "steganos" yang artinya adalah tulisan tersembunyi. Secara umum, steganografi adalah ilmu dan seni menyembunyikan informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Pesan-pesan tersebut dapat berupa teks, gambar, audio, video.

Steganografi berbeda dari kriptografi dan dapat dianggap sebagai pelengkap kriptografi, bukan pengganti. Hal ini karena steganografi menyembunyikan keberadaan pesan sehingga menghindari kecurigaan, sedangkan kriptografi menyembunyikan isi pesan sehingga pesan tidak dapat dibaca.

Metode yang paling umum digunakan untuk mengolah *cover* pesan berupa gambar adalah dengan teknik LSB. Teknik ini mengubah LSB pada gambar *cover* dengan bit data pesan rahasia.

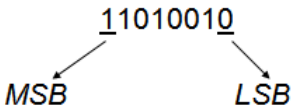


Fig. 1 MSB (*Most Significant Byte*) dan LSB

Pengubahan bit LSB hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya sehingga tidak berpengaruh terhadap persepsi visual/ auditori. Misalnya penyisipan pada citra 24-bit. Setiap piksel panjangnya 24 bit (3 x 3 *byte*, masing-masing komponen *R* (1 *byte*), *G* (1 *byte*), dan *B* (1 *byte*))

00110011 10100010 11100010
dengan pesan : **010**
Maka hasilnya adalah

00110010 10100011 11100010

Dari hasil tersebut dapat dilihat bahwa piksel berwarna merah hanya berubah sedikit dan tidak dapat dibedakan secara visual dengan citra aslinya karena pergeseran warna sebesar 1 dari 256 warna tidak dapat dilihat oleh mata manusia. Untuk metode ini, ukuran data yang dapat disembunyikan bergantung pada ukuran *cover-object* (obyek yang menjadi *cover*).

Untuk memperkuat teknik ini, bit-bit data rahasia tidak digunakan untuk mengganti *byte-byte cover* yang berurutan, namun dipilih susunan *byte* secara acak. Pembangkitan bilangan acak tersebut menggunakan PRNG (*Pseudo-Random Number Generator*). Umpan (*seed*) untuk bilangan acak berlaku sebagai kunci.

Pesan yang disembunyikan di dalam citra dapat diungkap kembali dengan mengekstraknya. Posisi *byte* yang menyimpan bit pesan dapat diketahui dari bilangan acak yang dibangkitkan PRNG. Jika kunci pada waktu ekstraksi sama dengan penyisipan, maka bilangan acak yang dibangkitkan juga sama sehingga bit-bit rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

III. KRIPTOGRAFI VISUAL

Kriptografi Visual adalah bentuk khusus metode kriptografi untuk menyembunyikan pesan dalam gambar sedemikian rupa sehingga dapat didekripsi oleh sistem visual manusia jika kunci gambar yang tepat digunakan. Tekni ini diajukan oleh Naor dan Shamir pada tahun 1994. Kriptografi Visual menggunakan minimal 2 buah gambar yang memiliki transparansi. Gambar satu berisi piksel acak dan sisanya berisi informasi rahasia . Tidak mungkin memperoleh informasi rahasia dari salah satu gambar.

Sistem Kriptografi Visual ini mirip dengan *one-time pad* dalam hal bahwa tiap halaman cipherteks didekripsikan dengan transparansi yang berbeda. Karena kesederhanaannya, sistem ini dapat digunakan oleh siapa saja tanpa pengetahuan apapun dalam kriptografi dan tanpa melakukan perhitungan kriptografi apapun.

A. Model

Cara paling sederhana dari pembagian gambar rahasia mengasumsikan pesan terdiri dari kumpulan piksel hitam dan putih dan tiap piksel ditangani secara terpisah. Tiap piksel original ditampilkan dalam bentuk modifikasi *n* (disebut bagian), satu untuk tiap transparensi. Tiap bagian adalah kumpulan dari *m* subpiksel hitam dan putih yang dicetak sedemikian rupa sehingga sistem visual manusia menyamakan kontribusi hitam/ putih masing-masing piksel tersebut.

Struktur hasil dapat dideskripsikan sebagai *n* x *m* matriks Boolean $S = [s_{ij}]$ dimana $s_{ij} = 1$ jika dan hanya jika subpiksel ke *j* dalam transparansi ke *i* adalah hitam. Ketika transparansi $i_1, i_2, \ldots, i_r$ ditumpuk satu sama lain secara tepat, kita dapat melihat kombinasi bagian subpiksel hitam yang direpresentasikan dengan Boolean

"OR" pada baris i_1, i_2, ..., i_r pada S. Tingkat abu-abu kombinasi bagian ini proporsional dengan berat Hamming H(V) dari *m* vektor V yang dikenai "OR". Tingkat abu-abu ini diinterpretasikan dengan sistem visual pengguna sebagai hitam jika$H(V) \geq d$ dan putih jika $H(V) < d - \alpha.m$ untuk beberapa tenggang $1 \leq d \leq m$ dan perbedaan relatif $\alpha > 0$.

Framework ini menunjukkan framework kode linear dengan perbedaan penting bahwa struktur algebranya adalah semigrup daripada sebuah grup. Khususnya, efek visual dari subpiksel hitam dalam salah satu transparansinya tidak dapat di *undo* dengan warna subpiksel dalam transparansi lain yang ditumpuk di atasnya. Hal ini menunjukkan teknik enkripsi umum yang menambah *noise* acak ke clearteks (plainteks) selama proses enkripsi, dan menghasilkan *noise* yang sama dari cipherteks selama proses dekripsi.

Hal ini juga menunjukkan model asli di mana piksel putih direpresentasikan dengan kumpulan subpiksel putih dan piksel hitam direpresentasikan dengan kumpulan subpiksel hitam sehingga kita harus menggunakan batas *d* dan perbedaan relatif $\alpha > 0$ untuk membedakan antar warna.

Solusi untuk *k* dari *n* skema pembagian visual rahasia terdiri dari dua kumpulan *n* x *m* matriks Boolean C_0 dan C_1. Untuk membagi piksel putih, dipilih secara acak salah satu matriks dalam C_0, dan untuk membagi piksel hitam dipilih secara acak salah satu dari matriks dalam C_1. Matriks yang dipilih mendefinisikan warna dari *m* subpiksel dalam tiap *n* transparansi. Solusi dianggap valid jika ketiga kondisi di bawah ini terpenuhi.

1. Untuk tiap S dalam C_0, "OR" V untuk tiap *k* dari baris *n* memenuhi $H(V) \leq d - \alpha.m$.
2. Untuk tiap S dalam C_1, "OR" V untuk tiap *k* dari baris *n* memenuhi $H(V) \geq d$.
3. Untuk tiap subset $\{i_1, i_2, ..., i_r\}$ dari {1, 2, …, *n*} dengan $q < k$, dua kumpulan matriks *q* x *m* D_1 untuk $t \in \{0, 1\}$ didapat dengan membatasi tiap matriks n x m dalam C_t (di mana $t = 0, 1$) ke baris i_1, i_2, ..., i_r dapat dibedakan dalam hal berisi matriks yang sama dengan frekuensi yang sama.

Kondisi 3 berarti dengan memeriksa lebih sedikit dari *k* bagian, bahkan seorang kripanalis yang sangat hebat tidak dapat memperoleh keuntungan dengan memutuskan apakah piksel yang dibagi adalah hitam atau putih. Dalam kebanyakan konstruksi, ada fungsi f untuk bagian yang terkombinasi dari $q < k$ transparansi berisi semua H(V) = f(*q*) dengan distribusi probabilitas *uniform*, tanpa melihat apakah matriks diambil dari C_0 atau C_1. Skema ini disebut *uniform*. Dua kondisi pertama disebut *contrast* dan kondisi ketiga disebut *security*. Parameter penting dari sebuah skema adalah :

- *m*, jumlah piksel dalam sebuah bagian. Hal ini merepresentasikan hilangnya resolusi dari gambar asli ke bentuk yang terbagi. Tentu saja kita menginginkan *m* sekecil mungkin.
- α, perbedaan relatif dalam hal tinggi antara bagian yang dikombinasikan yang dihasilkan dari sebuah piksel putih dan piksel hitam dalam gambar asli. Hal ini merepresentasikan kehilangan dalam *contrast*. Kita ingin α sebesar mungkin.
- *r*, ukuran kumpulan C_0 dan C_1 . Log *r* merepresentasikan jumlah bit acak yang dibutuhkan untuk menghasilkan bagian-bagian dan tidak berpengaruh pada kualitas gambar

Hasilnya, kita memiliki sejumlah konstruksi untuk nilai khusus dari *k* dan *n*. Secara umum, kita memiliki konstruksi untuk *k* dari *k* masalah dengan $m = 2^{k-1}$ dan $\alpha = \frac{1}{2^{k-1}}$ dan kita memiliki bukti optimalitas skema ini. Untuk *k* dan *n* secara umum, kita memiliki konstruksi dengan $m = \log n \cdot 2^{O(k \log k)}$ dan $\alpha = \frac{1}{2^{\Omega(k)}}$

B. Solusi Efisien untuk k dan n kecil

2 dari *n* masalah pembagian visual rahasia dapat diselesaikan dengan kumpulan matriks *n* x *n* berikut :

C_0 = {semua matriks didapat dengan permutasi kolom $\begin{bmatrix} 100 & ... & 0 \\ 100 & ... & 0 \\ & ... & \\ 100 & ... & 0 \end{bmatrix}$}

C_1 = {semua matriks didapat dengan permutasi kolom $\begin{bmatrix} 100 & ... & 0 \\ 010 & ... & 0 \\ & ... & \\ 000 & ... & 1 \end{bmatrix}$}

Tiap satu bagian dalam C_0 atau C_1 adalah pilihan acak dari satu subpiksel hitam dan *n*-1 subpiksel putih. Tiap dua bagian piksel putih memiliki berat Hamming terkombinasi 1, di mana dua bagian dari per 1 piksel memiliki berat Hamming terkombinasi 2, yang tampak lebih gelap. Perbedaan visual di antara dua kasus semakin jelas jika kita tambahkan tumpukan bagian transparansi.

Masalah asli dari kriptografi visual adalah kasus khusus 2 dari 2 masalah pembagian visual rahasia. Hal ini dapat dipecahkan dengan dua subpiksel per piksel, tapi dalam prakteknya, hal ini dapat mengubah aspek rasio gambar asli.

Fig.2 Gambar bagian per piksel

Karena hal itulah maka disarankan untuk menggunakan 4 subpiksel yang disusun dalam *array* 2x2 di mana tiap bagian memiliki satu bentuk visual pada Fig.2. Sebuah piksel putih dibagi ke dalam dua *array* yang identik dari *list* ini, dan piksel hitam dibagi ke dalam dua *array* pelengkap dari *list* ini. Tiap bagian adalah hasil acak dari dua subpiksel hitam dan dua subpiksel putih, yang terlihat abu-abu. Ketika dua bagian ditumpuk bersama, hasilnya

adalah abu-abu (merepresentasikan putih) atau hitam (merepresentasikan hitam).

Kasus berikutnya adalah 3 dari 3 masalah pembagian visual rahasia, yang dapat diselesaikan dengan skema berikut:

C_0 = {semua matriks didapat dengan permutasi kolom $\begin{bmatrix}0011\\0101\\0110\end{bmatrix}$}

C_1 = {semua matriks didapat dengan permutasi kolom $\begin{bmatrix}1100\\1010\\1001\end{bmatrix}$}

Tiap enam bagian yang dideskripsikan oleh baris C_0 dan C_1 adalah tepat enam *array* 2x2 dari Fig.2. Tiap matriks baik C_0 atau C_1 berisi satu bagian horizontal, satu bagian vertical, dan satu bagian diagonal. Tiap bagian berisi seleksi acak dari dua subpiksel hitam, dan pasangan bagian dari satu matriks berisi seleksi acak dari satu subpiksel hitam biasa dan dua subpiksel hitam individu. Akhirnya, analisis dari satu atau dua bagian tidak dapat membedakan C_0 dan C_1. Tetapi, tumpukan dari tiga transparansi dari C_0 hanya ¾ hitam, di mana tumpukan dari tiga transparansi dari C_1 benar-benar hitam.

Skema berikut menggeneralisasi 3 dari 3 skema ini ke dalam 3 dari n skema untuk $n \geq 3$ secara acak. Anggap B adalah matriks n x (n-2) hitam yang hanya berisi 1, dan anggap I menjadi matriks n x n identitas yang berisi 1 pada diagonalnya dan 0 untuk sisanya. Anggap BI menandakan matriks n x (2n-2) yang didapat dari penggabungan B dan I, dan anggap c(BI) menjadi komplemen Boolean untuk matriks BI. Sehingga

C_0 = {semua matriks didapat dari permutasi kolom c(BI)}

C_1 = {semua matriks didapat dari permutasi kolom BI}

memiliki property sebagai berikut : tiap bagian berisi kumpulan n-1 subpiksel hitam dan n-1 subpiksel putih; tiap pasangan bagian memiliki n-2 subpiksel hitam dan dua subpiksel hitam; tiap tiga tumpukan pasangan bagian dari C_0 memiliki n subpiksel hitam, di mana tiap tiga tumpukan pasangan dari C_1 memiliki n subpiksel hitam.

C. Skema umum untuk k dari k

Sekarang akan dijelaskan dua konstruksi umum yang dapat menyelesaikan k dari k masalah pembagian visual rahasia dengan menggunakan subpiksel 2^k dan 2^{k-1}.

Konstruksi 1

Untuk mendefinisikan kumpulan matriks kita gunakan dua *list* vektor $J_1^0, J_2^0, \ldots, J_k^0$ dan $J_1^1, J_2^1, \ldots, J_k^1$. Anggap $J_1^0, J_2^0, \ldots, J_k^0$ menjadi vektor sepanjang k pada GF[2] dengan property tiap k-1 adalah linear independent terhadap GF[2], tetapi kumpulan semua vektor k tidak independen. Kumpulan ini dapat dengan mudah dikonstruksi. Anggap $J_1^1, J_2^1, \ldots, J_k^1$ menjadi vektor sepanjang k pada GF[2] dengan property bahwa mereka independen linear terhadap GF[2]. Tiap *list* mendefinisikan matriks k x 2^k S^t untuk $t \in \{0, 1\}$ dan kumpulan C_0 dan C_1 didapat dengan permutasi kolom matriks yang berkorespondensi dalam semua cara yang mungkin. Kita tandai kolom S^t dengan vektor sepanjang k pada GF[2]. Untuk $t \in \{0, 1\}$ anggap S^t didefinisikan sebagai berikut: $S^t[i,x] = < J_i^t, x >$ untuk tiap $1 \leq i \leq k$ dan tiap vektor x sepanjang k pada GF[2] di mana <x, y> menandakan produk dalam pada GF[2].

Konstruksi 2

Sekarang akan ditunjukkan skema yang agak lebih baik dengan parameter $m = 2^{k-1}$, $\alpha = 1/2^{k-1}$ dan $r = 2^{k-1}!$. Perhatikan kumpulan $W = \{e_1, e_2, \ldots, e_k\}$ dari k elemen dan anggap $\pi_1, \pi_2, \ldots, \pi_{2^k-1}$ menjadi *list* semua subset kardinalitas genap dan $\sigma_1, \sigma_2, \ldots, \sigma_{2^k-1}$ menjadi list semua subset W dengan kardinalitas ganjil.

Tiap *list* mendefinisikan matriks k x 2^{k-1} S^0 dan S^1 : untuk $1 \leq i \leq k$ dan $1 \leq j \leq 2^{k-1}$ anggap $S^0[i, j] = 1$ jika dan hanya jika $e_i \in \pi_j$ dan $S_1[i, j] = 1$ jika dan hanya jika $e_i \in \sigma_j$. Seperti konstruksi di atas, kumpulan C_0 dan C_1 didapat dari permutasi semua kolom dengan matriks yang berkorespondensi.

Dengan data-data di atas, didapat teorema :

Pada skema k dari k apapun $\alpha \leq \frac{1}{2^{k-1}}$ dan $m \geq 2^{k-1}$.

D. Skema umum untuk k dari n

Pada bagian ini ditunjukkan bagaimana mengubah skema k dari k ke k dari n. Anggap C adalah skema pembagian visual rahasia k dari k dengan parameter m, r, α. Skema C berisi dua kumpulan matriks Boolean k x m $C_0 = T_1^0, T_2^0, \ldots, T_k^0$ dan $C_1 = T_1^1, T_2^1, \ldots, T_k^1$. Asumsikan skema adalah *uniform*. Anggap H menjadi kumpulan fungsi l sehingga

1. V$h \in H$ kita memiliki h : {1...n} -> {1…k}
2. Untuk semua subset $B \subset \{1 \ldots n\}$ dengan ukuran k dan semua $1 \leq q \leq k$ probabilitas $h \in H$ mendapatkan q dengan nilai yang berbeda pada B adalah sama.

Kita mengonstruksi dari C dan H sebuah skema C' k dari n seperti berikut :

- Kumpulan dasar adalah $V = U$ x H
- Tiap $1 \leq t \leq r^l$ ditandai dengan sebuah vektor (t_1, t_2, …, t_l) di mana tiap $1 \leq t_i \leq r$
- Matriks S_t^b untuk $t = (t_1, t_2, \ldots, t_l)$ di mana $b \in \{0, 1\}$ didefinisikan sebagai $S_t^b[i, (j, h)] = T_{t_j}^b[h(i), j]$

Pembentukan H

Kita dapat membuat H dari kumpulan fungsi hash independen *k-wise*. Anggap H untuk nilai k apapun $x_1, x_2, \ldots, x_k \in \{1, \ldots, n\}$ variabel acak k didefinisikan dengan $X_1 = h(x_1)$, $X_2 = h(x_2)$, …, $X_k = h(x_k)$ untuk $h \in H$ yang dipilih acak adalah independen. Karena mereka independen, probabilitasnya sama untuk menghasilkan nilai q yang berbeda, tidak peduli apapun $x_1, x_2, \ldots, x_k$ -nya. Untuk tiap

n dan k ada skema pembagian visual rahasia dengan parameter $m = n^k \cdot 2^{k-1}$, $\alpha = (2e)^{-k} / \sqrt{2\pi k}$ dan $r = n^k(2^{k-1}!)$.

IV. PENGUJIAN

Untuk pengujian digunakan aplikasi kriptografi visual berbasis web pada situs http://mars.banaan.org/vck/. Dalam situs ini kita dapat mengunggah gambar yang akan dienkripsi dan kemudian situs tersebut akan memunculkan hasilnya.

Sebagai contoh, dimasukkan gambar berikut sebagai gambar yang akan dienkripsi.

Fig.3 Gambar asli yang diuji

Dari hasil enkripsinya, dihasilkan dua gambar yaitu

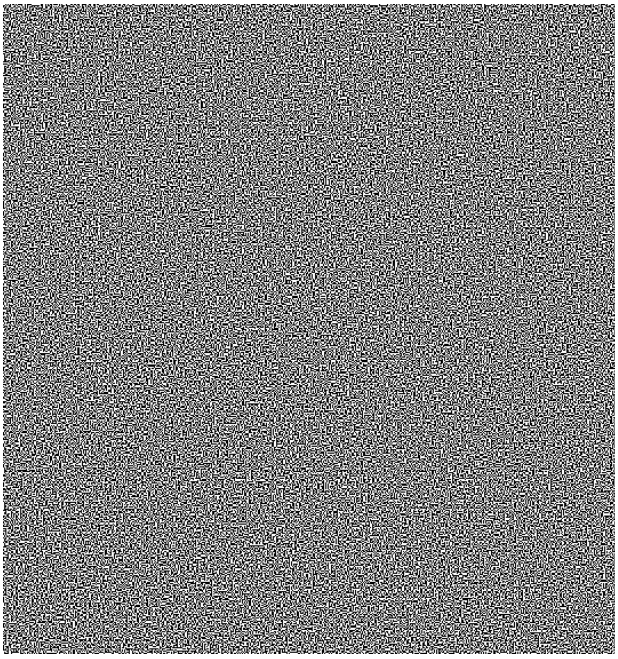


Fig.4 Gambar hasil enkripsi pertama

Dan,

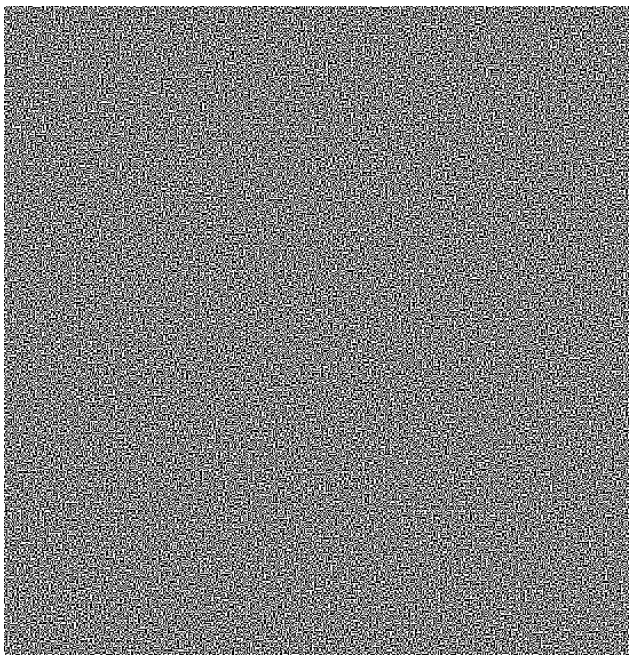


Fig.5 Gambar hasil enkripsi kedua

Hasil yang diperoleh jika kedua gambar hasil enkripsi tersebut ditumpuk adalah

Fig.6 Gambar hasil dekripsi

Dari gambar di atas dapat dilihat bahwa hasil dari penggunaan teknik kriptografi visual mengubah tampilan gambar asli baik dari segi warna, ukuran, dan resolusi.

Jika enkripsi diatur untuk menghasilkan gambar hasil enkripsi lebih banyak (lebih dari 2) maka penumpukan gambar hasil enkripsi tersebut mungkin tidak akan menampilkan gambar yang berarti jika hanya dilakukan penumpukan sebanyak 2 atau 3 gambar. Dekripsi yang maksimal hanya dapat dicapai jika semua gambar hasil

enkripsi ditumpuk tepat satu sama lain.

Pada percobaan pada situs lain, tidak hanya gambar yang dapat dikenai enkripsi ini. Pada situs tersebut pengguna diminta menuliskan pesan, dan akan mengeluarkan hasil enkripsi berupa gambar. Jika didekripsikan maka pesan awal yang dituliskan akan muncul pada gambar tersebut.

Pada percobaan lainnya, digunakan gambar dengan warna-warna yang mencolok. Ketika didekripsi, gambar tersebut bahkan tidak menampilkan gambaran besar dari gambar aslinya, dengan kata lain hasilnya tidak bagus.

V. Analisis

Dari hasil percobaan, dapat dilihat bahwa hasil dekripsi tidak akan menghasilkan gambar yang tepat sama seperti gambar asli. Hal ini dikarenakan pada proses enkripsinya terdapat *noise* yang disimpan pada gambar tersebut sehingga pada dekripsi, *noise* tersebut akan tetap muncul.

Perubahan resolusi, warna, *contrast* yang terjadi disebabkan oleh penggunaan jumlah bit-bit untuk melakukan enkripsi. Jika bit-bit yang digunakan berukuran besar, maka gambar yang dihasilkan dapat jadi besar. Pengolahan pada contoh di atas menghasilkan gambar hitam putih dan hilangnya warna dari gambar asli. Dari sumber-sumber lain ternyata ada juga modifikasi enkripsi yang masih dapat menghasilkan gambar berwarna meski gambar tersebut tidak persis sama.

Dari prinsip kerjanya, *watermarking* dapat diterapkan bersama kriptografi visual ini yaitu data-data *watermarking* disimpan dalam bagian-bagian gambar yang dienkripsi menggunakan kriptografi visual. Hal ini menambah keamanan dan menjamin keaslian dokumen.

Sampai sekarang tidak ada yang dapat memecahkan hasil enkripsi kriptografi visual ini karena seseorang tidak dapat melakukan apapun dengan hanya sebagian gambar hasil enkripsi. Hal ini karena pembangkitan bit hitam putih pada gambar dapat saja dibangkitkan secara acak.

VI. Konklusi

- Kriptografi Visual standar tidak cocok digunakan untuk data gambar yang menganggap penggunaan warna sangat penting.
- Gambar yang dikenai enkripsi menggunakan kriptografi visual, jika didekripsi tidak akan dapat menghasilkan gambar aslinya kembali.
- Enkripsi menggunakan kriptografi visual sangat aman dan tidak dapat dipecahkan
- Penggunaan dekripsi kriptografi visual sangat mudah
- Penerapan kriptografi visual dapat dikombinasikan dengan *watermarking*

Referensi

Barak, Boaz. 2007. Lecture-18 Secret Sharing, Visual Cryptography, Distributed Signature.

Baumgart, Matthias. 2003. Visual Cryptography. Chemnitz.

Hassan, Mahmoud A.; Khalili, Mohammed A. 2005. Self Watermarking Based on Visual Cryptography.

Naor, Moni; Shamir, Adi. 1998. Visual Cryptography. Springer-Verlag.

Surekha, B; Swamy GM; Rao, Srinivasa,dkk. A Watermarking Technique based on Visual Cryptography.

Http://it.toolbox.com/blogs/visual-cryptography/what-is-visual-cryptography-32240

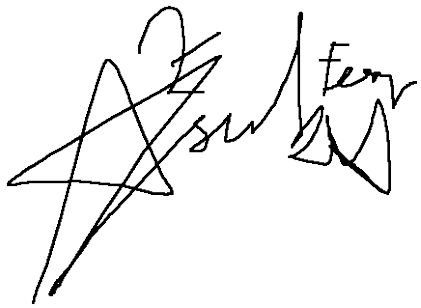
Http://rijmenants.blogspot.com/2008/01/Visual-cryptography.html

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

ttd



Franciscus Borgias Dian Paskalis - 13507048