Penggunaan Ide Visual Kriptografi dalam Pengenkripsian Multimedia

Eric Christopher / 13509037
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
Eric.c13@students.itb.ac.id

***Abstract*: Multiedia yang dimaksud disini adalah baik itu lagu (suara saja) maupun video. Kemudian akan ada usulan penggunaan visual kriptografi dengan cara lain.**

***Index:* Kriptografi, Steganografi, Visual Kriptografi, Media.**

I. LATAR BELAKANG

Pemilihan topic makalah ini murni berdasarkan ketertarikan penulis dengan visual kriptografi. Karena sekarang masih lebih menggunakan kriptografi modern seperti yang menggunakan kunci baik secret key, public key, maupun privat key, padahal dengan visual kriptografi kita hanya perlu mengetahui bagaimana cara membaca pesan dari share-share yang dia miliki dan tidak perlu menyimpan kunci.

Mungkin secara harafiah teknik visual kriptografi ini lebih cocok disebut steganografi daripada kriptografi, karena teknik ini lebih ke menyembunyikan pesan agar tidak terlihat dengan memecahnya menjadi beberapa share dan hanya dibutuhkan suatu teknik khusus untuk membacanya dan sesuai dengan namanya dapat dibaca hanya dengan visual saja.

Media yang dimaksudkan disini adalah semacam video yang merupakan gambar bergerak yang juga ada suara, maupun suara (mungkin bisa juga lagu atau musik dimasukkan di sini).

Mengapa dipilih audio dan video karena untuk gambar sudah ada teknik visual kriptografi yang dikembangkan walaupun sekarang masih dalam tahap pengembangan untuk menemukan yang lebih baik dan mengandung sedikit noise.

Audio atau suara dipilih karena dalam audio sendiri juga diperlukan sebuah teknik untuk penyisipan pesan dan dalam hal ini pesan yang disisipkan adalah pesan audio.

Video karena selain gambar dan audio media yang sering kita gunakan adalah video yang merupakan gabungan dari keduanya.

Yang ditekankan di makalah ini adalah ide dari visual kriptografi dimana orang yang ingin membaca pesan tadi tinggal "menggabungkan" share-share dari pesan yang dia miliki.

II. DASAR TEORI

Pertama-tama dalam makalah ini akan dijelaskan apa itu visual kriptografi. Karena sepertinya dalam dunia kriptografi sendiri ini masih jarang dikenal ataupun berkembang. Sekarang lebih sering dikembangkan tentang kriptografi sebagai segi keamanan informasi.

Untuk lebih jelasnya pertama-tama kita akan berbicara dulu tentang kriptografi, kriptografi adalah ilmu (ada juga beberapa sumber yang mengatakan bahwa kriptografi adalah sebuah seni) yang mempelajari bagaimana caranya untuk merahasiakan sebuah pesan. Dalam prakteknya kriptografi juga menyinggung beberapa aspek keamanan (contoh yang sudah ada adalah tentang bagaimana pertimbangan-pertimbangan dalam pembuatan digital signature) yaitu:

→ Kerahasiaan
tentu karena tujuan utama dari ilmu kriptografi ini sendiri adalah merahasiakan pesan agar tidak bisa dibaca oleh orang yang tidak seharusnya menerima pesan tersebut.

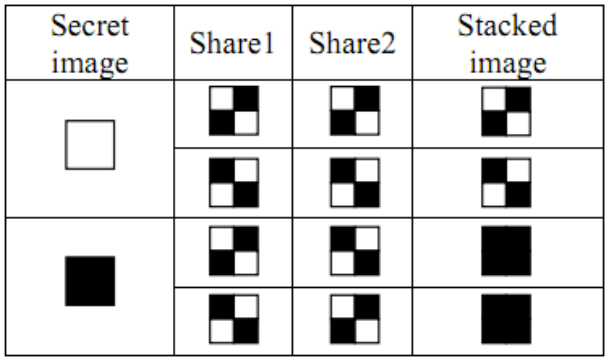
→ Integritas
dalam hal ini adalah menyakinkan apakah data tersebut masih asli atau dengan kata lain masih belum ada yang merubahnya.

→ Autentikasi
data tadi harus mengandung tentang identitas dari pengirimnya (jika diandaikan digital signature berarti tahu sumber dari pesan tadi dan bisa memastikan apakan pesan tersebut benar-benar dari dia).

→ Non-repudiasi
adalah metode agar si pengirim tidak dapat membantah bahwa data atau pesan tadi berasal dari dia.

Adapun jenis kriptografi lain yang diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1995. Kriptografi visual ini menggunakan media yang dapat dicetak, misalkan gambar atau citra. Pertama-tama Moni Naor dan Adi Shamir menggunakan citra biner dalam paper yang mereka buat, tetapi mereka juga memberikan kemungkinan pada warna abu-abu. Adapun yang mengatakan bahwa

algoritma dalam pembuatan visual kriptografi ini tidak membutuhkan perhitungan matematika dalam pendekripsiannya namun menggunakan pandangan mata belaka.



Sharing and stacking scheme of black and white pixels.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

Dengan menggunakan teknik 1 pixel dipecah menjadi empat buah pixel yang lebih kecil dan kemudian dengan menggunakan fungsi XOR untuk melihat hasilnya.

Terdapat juga sumber dari sebuah penelitian yang diambil dari link :

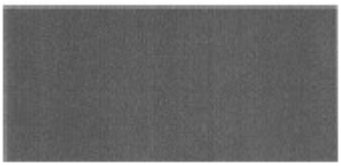
http://www.cs.fsu.edu/research/reports/TR-001001.pdf

bahwa visual kriptografi ini sendiri juga bisa diterapkan pada dokumen tentang financial. Mereka menamakan program yang mereka buat VCRYPT. Pada dasarnya idenya sama dengan ide tentang visual kriptografi yang pertama kali dikemukakan oleh Moni Naor dan Adi Shamir.

Share 1

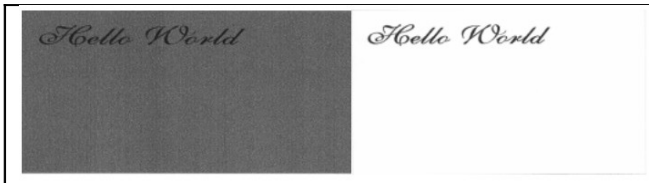
Sumber : http://www.cs.fsu.edu/research/reports/TR-001001.pdf

Share 2



Sumber : http://www.cs.fsu.edu/research/reports/TR-001001.pdf

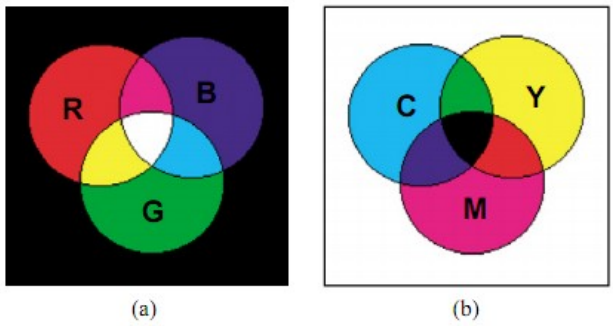
Ketika digabungkan akan menjadi tabel berikut.



Sumber : http://www.cs.fsu.edu/research/reports/TR-001001.pdf

Gambar di sebelah kiri adalah setelah dienkripsi dengan VCRYPT kemudian digabungkan kembali sedangkan sebelah kanan adalah gambar yang asli. Terdapat perbedaan yaitu terlihat seperti buram teteapi masih dapat terbaca.

Adapun sumber dari sebuah penelitian tentang visual kriptografi ini untuk gambar berwarna yang dilakukan Young-Chang Hou pada tahun 2002. Dalam paper tersebut ia menjelaskan bahwa untuk gambar berwarna terdapat dua buah jenis warna. Hal yang sama juga dijelaskan di mata kuliah sistem multimedia IF-STEI-ITB. Kedua jenis tersebut adalah additive dan subtractive. Additive adalah warna yang bila intensitasnya ditambahkan dengan jumlah yang merata akan menghasilkan warna putih (sering digunakan pada bahasa pemrograman maupun warna pada website ataupun pada alat-alat yang sering kita gunakan) terdiri atas merah, hijau dan biru (atau biasa disebut dengan RGB → Red, Green, Blue). Sedangkan model subtractive adalah pasangan warna yang bila ditambahkan intensitasnya dengan jumlah yang merata akan menjadi warna hitam (biasa digunakan di pewarnaan pada printer) yang terdiri atas warna cyan, magenta, dan yellow (biasa disebut CMYK → Cyan, Magenta, Yellow, dan blacK).



(a) Additive model, and (b) Subtractive model.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

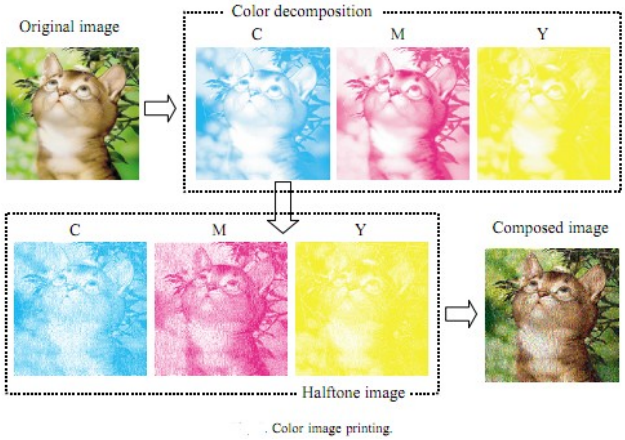
Di dalam papernya, Young memberikan beberapa teknik dalam pemakaian visual kriptografi untuk gambar berwarna. Kedua teknik yang dia tuliskan memanfaatkan tipuan mata ataupun kelemahan dari mata manusia. Yang pertama tekniknya tetap membagi 1 pixel menjadi 4 buah pixel kecil. Setiap blok pasti memiliki 2 buah pixel transparan dan digabungkan dengan blok mask. Berikut adalah tabel XOR dari gabungan beberapa share yang dia buat.

Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Scheme 1 of color cryptography.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

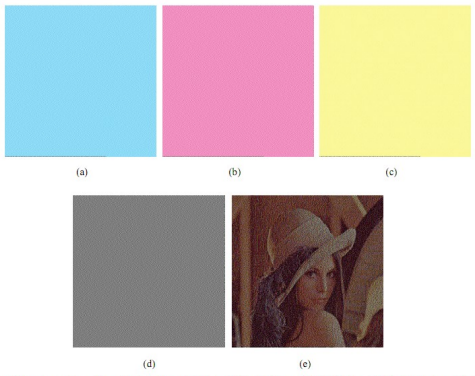
Memang jika dilihat dari tabel perbedaannya akan kelihatan jelas, akan tetapi bila ukurannya merupakan pixel maka gambar hasilnya masih tetap bisa dibaca. Seperti gambar kucing berikut.



. Color image printing.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

Berikut adalah percobaannya dengan menggunakan gambar lena dan ternyata untuk gambar tertentu metode ini kurang bagus digunakan.



Four separating shared transparencies and result of stacking: (a) Share 1(C), (b) Share 2(M), (c) Share 3(Y), (d) Mask, and (e) stacked image.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

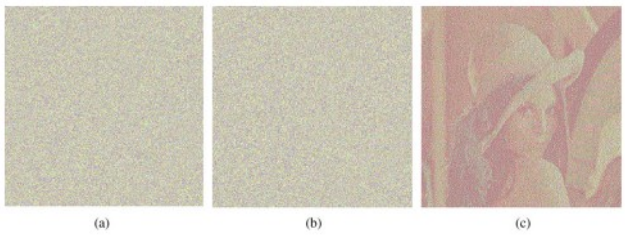
Karena hanya terdapat 8 jenis warna yang bisa dihasilkan dari teknik pertama maka dia juga mengembangkan teknik kedua yaitu sama-sama memecah satu buah pixel menjadi 4 pixel yang lebih kecil, namun pada prakteknya 4 buah pixel tadi akan ditumpuk (cyan, magenta, yellow, tranparan). Berikut adalah tabel dari teknik kedua.

Revealed color (C,M,Y)	Share 1	Share 2	Stacked image	Method	Resultant result	Revealed color quantity (C,M,Y)
(0, 0, 0)				Share 1and Share 2 with the same permutation		(1/4, 1/4, 1/4)
(1, 0, 0)				Swap the position of cyan and transparent		(1/2, 1/4, 1/4)
(0, 1, 0)				Swap the position of magenta and transparent		(1/4, 1/2, 1/4)
(0, 0, 1)				Swap the position of yellow and transparent		(1/4, 1/4, 1/2)
(1, 1, 0)				Swap the position of cyan and magenta		(1/2, 1/2, 1/4)
(0, 1, 1)				Swap the position of yellow and magenta		(1/4, 1/2, 1/2)
(1, 0, 1)				Swap the position of cyan and yellow		(1/2, 1/4, 1/2)
(1, 1, 1)				Swap two positions in pair		(1/2, 1/2, 1/2)

Fig. 10. Scheme 2 for color visual cryptography.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

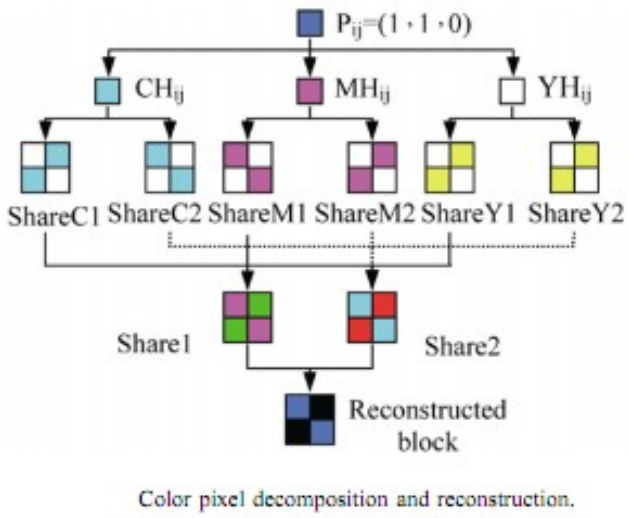
Berikut adalah hasil gambar lena yang sudah dienkripsi, terlihat bahwa gambar lena mengalami masalah di kekontrasan gambar sehingga masih susah juga untuk dilihat.



Two sharing transparencies and stacked effect: (a) Share 1, (b) Share 2, and (c) stacked image.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

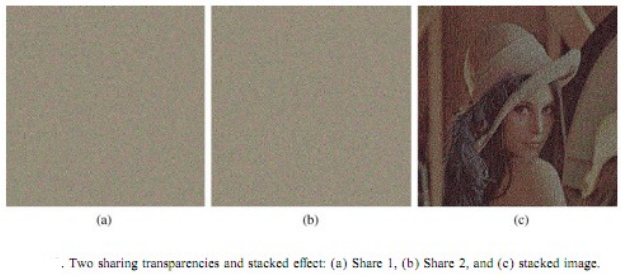
Terdapat satu metode lagi yang dikemukakan oleh Young, cara ini tidak begitu mengorbankan banyak kekontrasan dalam hal warna seperti pada teknik yang kedua.



Color pixel decomposition and reconstruction.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

Kemudian hasil pengenkripsian dengan menggunakan gambar lena adalah seperti gambar dibawah ini.



. Two sharing transparencies and stacked effect: (a) Share 1, (b) Share 2, and (c) stacked image.

Sumber : http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

Multimedia itu banyak sekali jenisnya, dan di dalam makalah ini hanya akan dibahas dua yaitu video dan suara maupun musik.

Pertama-tama akan dibahas mengenai video. Video sebenarnya adalah gambar yang diganti terus-menerus dengan cepat sehingga mata manusia tidak dapat melihat perubahannya dan menganggapnya sebagai gambar yang bergerak. Pada dasarnya video terdiri dari banyak frame. Terdapat tiga jenis frame pada video, yaitu:

→ I-Frame
(I dari Intra) adalah frame yang benar disimpan apa adanya, pixel per pixel disimpan utuh apa adanya (seperti menyimpan sebuah gambar utuh).

→ P-Frame
(P dari Predictive) adalah frame yang disimpan dengan menggunakan algoritma perubahan dari I-Frame sebelumnya.

→ B-Frame
(B dari Bi-directional) adalah frame yang diperkirakan dari I-Frame ataupun P-Frame sebelum dan sesudahnya.

Karena ketiga frame tersebutlah yang menyebabkan sewaktu kita menonton video dari youtube terdapat proses buffering karena dia masih menunggu mendapatkan Frame I maupun P setelahnya.

Berikutnya adalah suara, cara perekaman suara adalah dengan menggunakan sebuah membrane dan getaran dari membrane tadi akan didigitalisasi menjadi data yang bisa kita copy-copykan. Dengan kata lain yang disimpan adalah amplitude dari suatu sampel suara, dan banyaknya sampel yang akan diambil tergantung kualitas yang diinginkan (8000 per detik untuk telepon, 44100 untuk audio CD, 48000 untuk audio DVD, dan 192400 untuk HD-DVD/kualitas blue ray). Semakin banyak sampel yang diambil berarti semakin bagus kualitas dari audio atau suara itu sendiri. Adapun aturan untuk menentukan berapa sampel yang sebaiknya dipakai dalam penyimpanan suara, tetapi hal tersebut tidak akan dibahas pada makalah kali ini.

III. PEMBAHASAN

Karena di dalam makalah ini akan dibahas dua buah jenis media maka akan kita pecah dulu. Pertama –tama akan dibahas tentang audio terlebih dahulu, karena video juga mengandung audio.

Pada audio yang disimpan adalah amplitude dari sampel-sampel yang diambilnya. Pada bahasa java perekaman suara dapat dilakukan dengan mengambil sample yang ada dibuffer dari sebuah kelas line (kelas yang mengatur rekaman suara). Buffer tadi akan disimpan ke sebuah array of byte (buffer berisi amplitudo-amplitudo dari sampel).

Ide dari visual kriptografi adalah dengan menyatukan share-share dari sebuah gambar yang sudah dipecah untuk mendapatkan makna dari pesan secara visual. Dalam hal suara ini maka ide tadi bisa digunakan dengan cara menyimpan buffer tadi (buffer berisi amplitudo-amplitudo dari sampel) ke dalam file yang berbeda di tiap detiknya secara bergantian. Misal sampel dalam detik pertama akan disimpan di share pertama, kemudian detik kedua di share kedua, detik ketiga di share ketiga, detik ke keempat kembali disimpan pada ke share pertama, detik kelima pada share kedua, dan seterusnya seperti pada tabel berikut (misal dipisah ke dalam tiga share).

	Share 1	Share 2	Share 3
Detik	1	2	3
	4	5	6
	7	8	9
	10	11	12
	13	14	15

Penyimpanan ini tetap berbasiskan waktu sehingga karena detik pertama disimpan dishare pertama maka di share kedua dan ketiga detik pertamanya sunyi (tidak ada suara sama sekali). Kemudian hal yang sama juga terjadi pada detik kedua. Karena detik kedua disimpan pada share

kedua maka pada share pertama dan ketiga detik keduanya sunyi.

Hal pembagian ini kurang lebih sama seperti audio yang bertype stereo dimana sebenarnya adalah pemutaran dua buah lagu dalam channel berbeda (channel kanan dan channel kiri, bahkan untuk karaoke mungkin ada channel ketiga untuk suara penyanyinya). Jika saja diputar hanya salah satu channel maka music tadi kurang bisa terdengar dengan jelas, tetapi jika dimainkan semua channelnya maka akan menjadi music yang enak untuk didengar tanpa terasa padahal itu sebenarnya berasal dari dua buah atau lebih channel.

Tetapi jika langsung digunakan begitu saja maka kemungkinan akan menimbulkan kecurigaan karena akan terdengar suara putus-putus. Maka dari itu digunakanlah sebuah media lain yang berupa suara juga (misalkan sebuah music) dimana share pertama, kedua, dan ketiga akan digabungkan di music tadi dengan sedikit pengeditan (misal pengecilan amplitude agar tidak terlalu kelihatan mencolok ataupun peninggian amplitude agar pesan suara tadi tidak terlalu tertutup oleh music backgroundnya). Kemudian juga disarankan menggunakan music yang sama dalam penyisipan agar dapat dibaca. Kemudian penyisipannya juga harus pada detik yang sama agar share-share tadi saling melengkapi satu dengan yang lain. Misal bila share pertama disisipkan mulai detik ke 5 dari lagu maka hal yang sama juga harus diterapkan terhadap share kedua, share ketiga dan share-share berikutnya.

Kemudian cara membacanya adalah dengan cara memutar music yang mengandung share pertama, music yang mengandung share kedua, dan music yang mengandung share ketiga tadi secara bersamaan (mungkin dibutuhkan program tambahan untuk hal ini). Jika file music tadi diputar sendiri-sendiri maka hanya akan terdengar seperti noise di telinga kita (apalagi sewaktu penyisipan sudah diturunkan amplitudonya maka bisa tidak terdengar karena tertutup oleh music yang asli). Begitu pula jika mempunyai beberapa share tetapi tidak lengkap misalkan dua dari tiga buah share sehingga pesan yang ada hilang sepertiganya. Namun mungkin masih bisa dibaca dengan cara menebak-nebak pesan suara yang didengar, namun bisa jadi kurang akurat karena juga terdapat music background yang menutupi pesan tadi.

Hal yang mungkin akan menjadi pertimbangan di sini adalah tentang jenis music yang akan menjadi media penyusupan pesan tadi. Hal ini akan menjadi pertimbangan karena jika yang digunakan music semacam rock ataupun yang mengandung suara yang keras maka kemungkinan pesan yang akan disusupi akan tertutupi oleh music tersebut. Adapun range amplitude yang sebaiknya digunakan dalam penyisipan (pengaruh ke pengubahan amplitude sebelum penyusupan ke music yang akan disusupi).

Berikutnya kita akan berbicara tentang video. Video terdiri atas gambar dan suara. Untuk yang suara dapat digunakan cara seperti pengenkripsian suara tadi sesuai dengan banyak share video yang ada. Namun dalam hal ini tidak perlu diberi music karena akan merusak pesan video tersebut sendiri.

Untuk masalah gambarnya sendiri kata kuncinya adalah dari frame-frame yang ada di video yang sudah dijelaskan pada kajian teori. Pada dasarnya semua frame tadi tergantung dari I-Frame. Maka bila I-Framenya saja yang didekripsi maka seluruh isi video akan berubah. Hal ini disebabkan karena P-Frame merupakan perkiraan dari perubahan I-Frame, kemudian B-Frame adalah frame yang terbentuk dari pendekatan I-Frame ataupun P-Frame sebelumnya dan sesudahnya. Karena gambar di video kebanyakan adalah gambar berwarna maka perlu menggunakan teknik pengenkripsian seperti yang terdapat pada paper dari Young tentang visual kriptografi dalam gambar berwarna.

Jadi dalam sebuah video akan dipecah menjadi n buah video yang terpecah-pecah Frame I-nya kemudian untuk suara bisa juga dipecah seperti dalam pemecahan suara tadi.

Akan tetapi masalah yang muncul adalah bagaimana menyatukan video-video tadi agar bisa dilihat, karena video bukanlah seperti gambar biasa yang bisa langsung diprint. Adapun cara yang terpikir adalah dengan menggunakan beberapa proyektor untuk memproyeksikan video tadi agar bisa ditumpuk satu dengan yang lainnya untuk mendapatkan video yang asli. Namun cara ini memiliki kelemahan yaitu gambar yang ada di layar komputer (gambar sebenarnya) dengan gambar yang diproyeksikan kemungkinan mengalami perbedaan, maka dari itu bisa jadi gambarnya akan lebih susah dibaca daripada aslinya.

Sesuai dengan perkembangan jaman maka teknologi juga berkembang, sekarang sudah banyak sekali kita lihat tentang pengembangan Augmentation Reality yang dimana memungkinkan kita untuk melihat sebuah video tanpa menggunakan apapun (untuk lebih jelasnya banyak sekali video di youtube yang menjelaskan tentang hal ini). Ada yang memiliki ide dengan menggunakan hologram ada juga dengan menggunakan proyektor. Dengan perkembangan teknologi yang seperti itu tadi maka penggabungan beberapa video ini bukanlah menjadi masalah.

IV. KESIMPULAN

Kesimpulan yang dapat diambil adalah dalam pengembangannya visual kriptografi ini masuk termasuk muda dan masih dapat berkembang lebih lanjut. Untuk visual kriptografi sendiri masih belum ditemukan algoritma yang bagus untuk memecah sebuah gambar berwarna agar ketika digabungkan hanya memiliki sedikit noise dan menggunakan algoritma yang tidak begitu membutuhkan perhitungan yang besar ataupuntidka lama dalam pembuatan sharenya.

Perkembangan teknologi juga dapat memudahkan

ataupun menjadi inovasi bagi perkembangan selanjutnya (contohnya tentang Augmentation Reality atau yang biasanya disingkat dengan AR).

Suara dapat dipecah dengan cara memecahnya per interval waktu sesuai dengan banyak share yang diinginkan, kemudian menyisipkan atau menyembunyikannya ke sebuah music yang sama dan dimulai dalam waktu yang sama (agar bisa digabungkan dengan cara memainkan semua sharenya secara bersama-sama).

Video sebenarnya merupakan gabungan dari gambar serta suara. Untuk suaranya dapat dilakukan seperti teknik yang dibicarakan sebelumnya namun tidak disembunyikan pada sebuah file audio yang lainnya. Untuk gambarnya sendiri dapat dilakukan pemecahan pada semua Frame I-nya sehingga secara otomatis semua frame akan berubah dan tidak bisa dibaca.

Dalam penyatuannya teknologi sekarang bisa menggunakan beberapa proyektor yang menampilkan masing-masing share dan disorotkan ketempat yang sama serta dimainkan secara bersamaan.

Untuk yang suara dapat juga dilakukan penelitian tentang seberapa tinggi amplitude dari pesan yang disisipkan beserta jenis music yang bagus untuk dijadikan media penyisipan. Hal tadi dapat memberikan semacam batasan ataupun aturan dalam pembuatan share-share dari pesan suara agar mendapatkan metode pengenkripsian yang lebih baik.

Kemudian juga dapat dilakukan penelitian tentang berapa share yang sebaiknya digunakan untuk mendapatkan hasil yang bagus atau optimal (dilihat dari berbagai sudut pandang seperti keamanan, kecurigaan, banyaknya share).

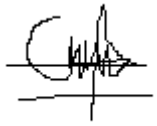
DAFTAR PUSTAKA

[1] Slide Kriptografi ITB 2012
[2] Slide Sistem Multimedia ITB 2012
[3] http://www.youtube.com
[4] http://darto2008.blogspot.com/2009/04/kriptografi-visual.html
[5] http://digilib.itb.ac.id/gdl.php?mod=browse&op=read&id=jbptitbpp-gdl-muhamadari-29915
[6] http://www.cs.fsu.edu/research/reports/TR-001001.pdf
[7] http://www.colorimageprocessing.com/research_secureimaging1.htm
[8] http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf

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, 1 Mei 2012



Eric Christopher / 13509037