Studi *Extended Visual Cryptography Schemes* dan Kontribusinya Dalam Kehidupan

Imam Prabowo K (13507123)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
imam.prabowo.k@gmail.com
if17123@students.if.itb.ac.id

Abstrak - Kriptografi visual adalah teknik enkripsi gambar yang membuat pesan citra rahasia (*hidden image*) ke dalam beberapa transparansi gambar (*share*) yang tidak memiliki arti, kemudian gambar tersebut dapat dengan mudah didekripsi hanya mengandalkan visual manusia tanpa menggunakan kalkulasi tertentu. Teknik ini sangat sederhana karena penerima dapat dengan mudah membaca *hidden image* tanpa menggunakan sebuah kunci atau algoritma dekripsi. Teknik kriptografi visual juga sangat aman dari serangan kriptanalisis karena *share* yang dibangkitkan benar-benar acak menggunakan kunci asimetri, sehingga memiliki konsep *one-time pad* yang secara absolut tidak bisa didekripsi kecuali jika penerima memiliki seluruh *share* yang cukup diperlukan untuk menampilkan *hidden image* [1].

Teknik kriptografi visual pertamakali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994 yang mengubah *hidden image* menjadi minimal n buah *share*, kemudian *hidden image* hanya dapat dibaca kembali jika n buah *share* tersebut diletakkan tepat di atas satu dan lainnya. Skema kriptografi tersebut diberi nama *Visual Secret Sharing Scheme* (VSSS) [1]. Kemudian konsep ini terus berkembang dengan diperkenalkannya konsep (k, n)-*threshold* [1] dan *general access structure* [2].

VSSS kemudian dikembangkan kembali karena pada aplikasinya terdapat beberapa masalah terkait kualitas gambar yang mengandung titik-titik acak sehingga menimbulkan kecurigaan pada *share* yang dibangkitkan dari *hidden image*. Hal ini merupakan latar belakang diperkenalkannya teknik *Extended Visual Cryptography Scheme* (EVCS) yang merahasiakan tiap-tiap subset dari *share* ke dalam bentuk gambar yang mengandung makna (bukan lagi berbentuk titik-titik acak) sehingga perpaduan antar*share* dapat menipu penerima jika tidak memiliki sejumlah *share* tertentu untuk membangkitkan kembali *hidden image* yang dimaksud [3].

Makalah ini akan mengkaji teknik EVCS, prinsip kerja, serta manfaat EVCS dalam penerapannya di kehidupan sehari-hari.

***Kata kunci: Extended Visual Cryptography Schemes* (EVCS), kriptografi visual, *hidden image*, *share*.**

I. PENDAHULUAN

Di era revolusi informasi ini, manusia di seluruh dunia semakin memanfaatkan teknologi informasi dalam aktivitas hidupnya sehari-hari. Pertukaran informasi melalui media seperti internet telah menjadi kebutuhan utama bagi setiap manusia. Seiring dengan semakin berkembangnya teknologi informasi, kebutuhan terhadap keamanan informasi semakin tinggi. Oleh karena itu seiring dengan berkembangnya teknologi informasi, ilmu kriptografi menjadi semakin dibutuhkan untuk melakukan penyandian informasi yang semakin kuat, aman, dan semakin mudah digunakan untuk berbagai model kasus yang beragam. Salah satu teknik kriptografi yang paling mudah digunakan dan memiliki keamanan yang cukup tinggi saat ini yaitu kriptografi visual.

Kriptografi visual adalah teknik enkripsi gambar yang membuat pesan citra rahasia (*hidden image*) ke dalam beberapa transparansi gambar (*share*) yang tidak memiliki arti, kemudian gambar tersebut dapat dengan mudah didekripsi hanya mengandalkan visual manusia tanpa menggunakan kalkulasi atau algoritma dekripsi tertentu. Teknik ini sangat memudahkan karena penerima dapat membaca *hidden image* tanpa menggunakan sebuah kunci atau algoritma dekripsi. Teknik kriptografi visual juga sangat aman dari serangan kriptanalisis karena *share* yang dibangkitkan benar-benar acak menggunakan kunci asimetri, sehingga memiliki kemiripan dengan konsep *one-time pad* yang secara absolut tidak bisa didekripsi kecuali jika penerima memiliki seluruh *share* yang dibutuhkan untuk menampilkan *hidden image* [1].

Teknik kriptografi visual pertamakali diperkenalkan oleh Moni Naor Adi Shamir pada tahun 1994 yang mengubah *hidden image* menjadi minimal n buah *share*, kemudian *hidden image* hanya dapat dibaca kembali jika n buah *share* tersebut diletakkan tepat di atas satu dan lainnya. Skema kriptografi yang diperkenalkan mereka diberi nama *Visual Secret Sharing Scheme* (VSSS) [1]. Kemudian konsep ini terus berkembang dengan diperkenalkannya konsep (k, n)-*threshold* [1] dan *general access structure* [2].

VSSS kemudian dikembangkan kembali karena pada aplikasinya terdapat beberapa masalah terkait kualitas

gambar yang mengandung titik-titik acak dari *share*, sehingga dapat menimbulkan kecurigaan pada *share* yang dibangkitkan dari *hidden image* karena dianggap sebagai gambar yang tidak memiliki arti. Hal ini menjadi latar belakang diperkenalkannya sistem *Extended Visual Cryptography Scheme* (EVCS) yang merahasiakan tiap-tiap subset dari *share* ke dalam bentuk gambar yang memiliki arti (bukan lagi berbentuk titik-titik acak) sehingga perpaduan antar*share* dapat menipu penerima dan tidak menimbulkan kecurigaan [3].

II. TEORI DASAR

A. *Visual Secret Sharing Scheme*

Visual Secret Sharing Scheme merup akan metode yang pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir. Metode ini merupakan metode yang paling sederhana dalam kriptografi visual. Citra dibagi menjadi 2 *share* yang terlihat tidak memiliki informasi. Untuk mendapatkan citra kembali atau dekripsi, kedua *share* harus ditumpuk menjadi satu. Cara ini dinilai sangat aman karena tidak satupun *share* mengandung sedikit pun informasi mengenai citra yang dirahasiakan, sekalipun secara implisit.

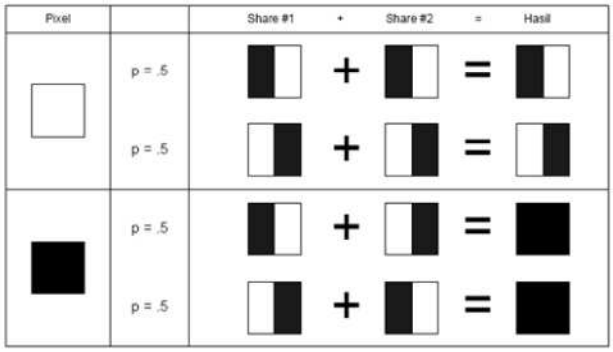
Share pertama pada *Visual Secret Sharing Scheme* didapatkan dari nilai random masing-masing pixel. Untuk gambar hitam putih (*binary image*), nilai random hanya berkisar antara dua nilai, yaitu hitam atau putih untuk setiap pixelnya. Hasil dari citra random ini adalah citra dengan warna hitam-putih yang tak beraturan. Setelah *share* pertama didapatkan, selanjutnya adalah membuat *share* kedua. *Share* kedua didapatkan dengan mempertimbangkan *share* pertama yang merupakan citra random. Setiap pixel pada *share* kedua dapat bernilai hitam ataupun putih bergantung pada kondisi berikut:

1. Jika pixel pada citra asli berwarna putih dan pixel pada *share* pertama berwarna putih, maka pixel pada *share* kedua juga bernilai putih.
2. Jika pixel pada citra asli berwarna putih sedangkan *pixel* pada *share* pertama berwarna hitam, maka pixel pada *share* kedua berwarna hitam.
3. Jika pixel pada citra asli berwarna hitam sedangkan pixel pada *share* pertama berwarna putih, maka pixel pada *share* kedua berwarna hitam.
4. Jika pixel pada citra asli berwarna hitam dan pixel pada *share* pertama berwarna hitam, maka pixel pada *share* kedua berwarna putih.

Aturan tersebut mirip seperti operasi logika "XOR" pada tabel kebenaran dengan anggapan warna putih adalah 0 dan warna hitam adalah 1.

Setiap pixel pada *share* pertama dan *share* kedua kemudian dibagi menjadi beberapa blok (subpixel) yang lebih kecil. Sama seperti pixel pada citra, subpixel hanya dapat berwarna hitam atau putih. Jumlah warna subpixel hitam dan putih ini akan selalu sama.

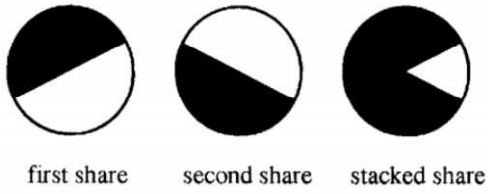
Contoh sederhana dari pembagian subpixel ini adalah dengan membagi tiap pixel menjadi 2 subpixel seperti gambar di bawah ini.



Gambar 1. Model kriptografi visual pada subpixel

Pada gambar di atas terlihat bahwa satu pixel terbagi menjadi 2 bagian, yaitu kanan dan kiri dengan 1 bagian berwarna putih dan bagian lainnya berwarna hitam. Ada 4 kemungkinan susunan yang dapat dibentuk dari 2 *share* dengan model 2 subpixel ini. Dari 4 kemungkinan tersebut, dapat disimpulkan bahwa pixel yang dihasilkan dari kedua *share* akan berwarna putih jika kedua *share* memiliki susunan warna subpixel yang sama, dapat berupa hitam di sebelah kiri dan putih di sebelah kanan maupun sebaliknya. Sedangkan pixel hitam didapatkan bila susunan warna subpixel pada kedua *share* berbeda, misalkan pada *share* 1 subpixel hitam berada di kiri dan pada *share* 2 subpixel hitam berada di sebelah kanan.

Selain dengan pemodelan pixel segi empat, pixel juga dapat digambarkan dengan ilustrasi lingkaran, dimana sudut yang terbentuk pada lingkaran merupakan tingkat keabuan pixel.



Gambar 2. Ilustrasi tingkat keabuan pada VSSS

B. *General Access Structure*

Metode *Visual Secret Sharing Scheme* juga dapat dikembangkan dengan metode *general access structure*. Jumlah *share* pada *General Access Structure* dapat lebih

dari 2 dan untuk membentuk kembali citra asal, belum tentu semua *share* diperlukan. Skema ini dikenal sebagai *k out of n scheme*, dimana terdapat n jumlah *share* dan untuk membentuk citra asli diperlukan sejumlah k *share*.

General Access Structure juga dapat mendefinisikan subset himpunan *share* tertentu yang terkualifikasi untuk menampilkan *hidden image* dan subset yang tidak dapat menampilkan *hidden image*. Berikut ini adalah sejumlah aturan dari *general access structure*:

1. Set partisipan : P = {1,2,…..,n}
2. Qualified set (G_{qual}), yaitu kumpulan beberapa *share* yang bila digabungkan dapat membentuk citra asal. G_{qual} adalah subset dari 2P.
3. Forbidden set (G_{forb}), yaitu kumpulan beberapa *share* yang bila digabungkan tidak akan membentuk citra asal.
4. Jika $G_{qual} \cap G_{forb} = 0$ maka (G_{qual}, G_{forb}) merupakan *General Access Structure Scheme*.

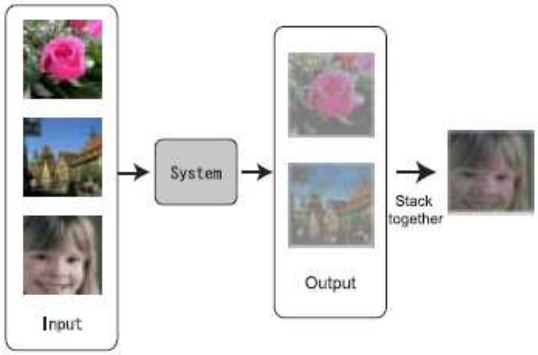
Pada skema ini, setiap satu pixel dari gambar rahasia yang dijadikan *hidden image* akan dipecah menjadi sebanyak m subpixel pada lembar trasparansi. Jika jumlah subpixel transparansi yang ditumpuk melebihi batas k, maka pixel tersebut dianggap "on" dan terlihat. Sedangkan bila jumlahnya masih di bawah k, maka pixel tersebut dianggap "off" dan tidak terlihat. Hofmeister juga telah mendiskusikan α dengan menggunakan pemrograman liner pada kasus k $\in$ {3, 4, n} yang menghasilkan gambar yang mirip dengan *hidden image* aslinya demgan nilai n tertentu.

C. *Extended Visual Cryptography Schemes*

Extended Visual Cryptography Schemes (EVCS) adalah sebuah teknik kriptografi visual untuk menyandikan sebuah *hidden image* ke dalam gambar-gambar bayangan sebanyak n, sedemikian hingga ketika kita menumpuk gambar tersebut secara bersamaan yang terasosiasi *qualified*, maka kita dapat melihat pesan rahasia. Sebaliknya, jika gambar yang bertumpuk terasosiasi *forbidden*, maka kita tidak dapat melihat *hidden image*, melainkan dapat melihat gambar lain yang masih bermakna, sehingga gambar transparansi yang dihasilkan (*share*) merupakan gambar tertentu yang tidak mencurigakan seperti titik-titik acak. Selain itu, kriptanalis dapat menyangka bahwa gambar kamuflase tersebut adalah pesan rahasia asli yang disembunyikan [3].

Skema EVCS berawal dari inspirasi pemanfaatan steganografi pada kriptografi visual, yang merupakan penyisipan *share* ke dalam sebuah gambar yang bermakna. Penyisipan *share* ini tidak menimbulkan kecurigaan pada pengamat karena secara kasat mata ia hanya melihat sebuah gambar tertentu yang memiliki makna, padahal di dalamnya terdapat *share* yang diperlukan untuk decode *hidden image* jika ditumpuk dengan *share* lainnya.

Gambar berikut ini merupakan ilustrasi dari EVCS.



Gambar 3. Ilustrasi ide dasar *Extended Visual Cryptography Schemes*

Ateniese et al telah memformalkan *framework Extended Visual Cryptography Schemes* (EVCS) sebagai pengembangan dari *Visual Secret Sharing Scheme* (VSSS) dan mengembangkan kembali skema *general access structure* dengan kombinasi konsep (k, n)-*threshold* [2].

EVCS, dalam *general access structure* (τ Qual; τ Forb) pada sebuah kelompok yang terdiri dari n partisipan gambar (*share*), dapat menyandikan sebanyak n gambar sedemikian hingga ketika kita menumpuk gambar tersebut secara bersamaan yang terasosiasi pada set X $\in \tau_{Qual}$, maka kita dapat melihat *hidden image*. Sebaliknya, jika gambar terasosiasi pada X $\in \tau_{Forb}$, maka yang akan muncul adalah gambar kamuflase yang bisa didefnisikan sebelumnya.

III. PRINSIP KERJA EVCS

A. Teori Fundamental EVCS

Kriptografi visual merupakan kriptografi yang berbasis operasi boolean. Oleh karena itu pemisahan rona pixel (*halftoning*) adalah hal yang dibutuhkan untuk pengaplikasian kriptografi visual pada gambar *grayscale*. Transparansi rata-rata pada sebuah pixel dalam konteks teknik *halftoning*.

Dengan Ω merepresentasikan daerah tertentu pada pixel dan t(x) adalah transparansi dari poin x dalam sebuah region, maka persamaan transparansi rata-rata dari Ω sesuai dengan sistem visual manusia adalah:

$$\frac{\int\Omega\ t(x)\ dA}{A\Omega}$$

Dimana fungsi integra menyatakan area dari Ω. Dengan t1(x) dan t2(x) adalah transparansi lembar 1 dan 2 pada poin x, transparansi dari pixel tersebut adalah t1(x).t2(x), sehingga transparansi rata-rata dari daerah Ω adalah:

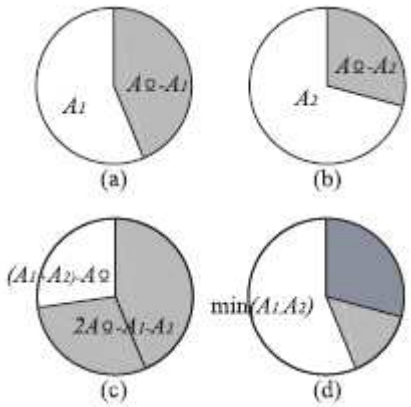
$$t\Omega = \frac{\int\Omega\ t1(x).t2(x)\ dA}{A\Omega}$$

Untuk gambar *grayscale* transparansi rata-ratanya menjadi:

$$t\Omega = \frac{AT}{A\Omega}$$

Dimana $A_T = \int\Omega\ t(x)\ dA$ menyatakan area dari transparansi (t(x) = 1) di region Ω.

Operasi yang terjadi saat kedua *share* bentuk biner ditumpuk secara tepat, product dari boolean direpresentasikan oleh gambar berikut:



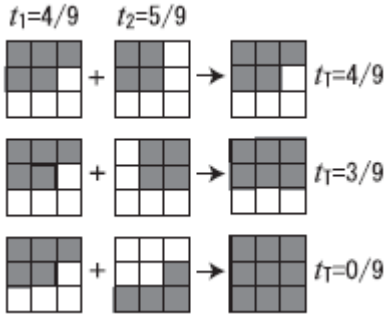
Gambar 4. Daerah *range* dari region transparansi target pixel.

Pada gambar 4 di atas, (a) A1 menyatakan transparansi region pada *share* 1, (b) A2 menyatakan transparansi region pada *share* 2, (c) dearah transparan diperoleh dari menumpuk *share* 1 dan *share* 2, sedangkan (d) menunjukkan merupakan daerah *gray* minimum dari A1 dan A2.

B. Proses EVCS

Teknik *halftoning* memiliki beberapa variasi. Algoritma *non-periodic and dot-dispersed dithering* merupakan algoritma yang paling cocok digunakan karena memungkinkan aransemen *low arbitrary subpixel*. Oleh karena itu, algoritma error-diffusion telah diadopsi.

Proses enkripsi terdiri dar menentukan aransemen dari subpixel transparan pada tiap lembar *share* berdasarkan transparansi pixel, t1, t2, dan tT seperti yang ditunjukkan oleh gambar di bawah ini.



Gambar 5. Contoh dari aransemen subpixel dengan $t_1 = 4/9$ dan $t_2 = 5/9$, $t_r = 4/9$ dapat didapat dengan mengaransemen subpixel pada contoh di atas.

Pada gambar di atas, satu pixel dalam gambar *grayscale* dilakukan *halftone* dengan m subpixel. Enkripsi dilakukan pada tiga gambar dari pixel ke pixel. Dengan s_1, s_2, dan s_T menyatakan angka dari subpixel transparan pada pixel di masing-masing lembar *share* 1, *share* 2 dan target. Transparansi pixel dari *share* dan target menjadi $t_1 = s_1/m$, $t_2 = s_2/m$, dan $t_T = s_T/m$. Komputasi enkripsi dapat dilakukan dengan pemodelan operasi product matriks dalam bentuk boolean. Dengan 0 menunjukkan transparansi 100% dan 1 menunjukkan *opaque*100%.

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

Tabel di bawah ini menunjukkan transparansi dari subpixel T_1, T_2, dan T_T dan angka dari tiap pasang.

subpixel transparency			number of
τ_1	τ_2	τ_T	subpixel pairs
1	1	1	P_{11}
1	0	0	P_{10}
0	1	0	P_{01}
0	0	0	P_{00}

$P_{T1,T2}$, m, s_1, s_2, dan s_T adalah:
$s_1 = P_{11} + P_{10}$
$s_2 = P_{11} + P_{01}$
$s_T = P_{11}$
$m = P_{11}+P_{01}+P_{10}+P_{00}$

Aransemen dari m subpixel dari tiap *share* ditentukan dari menyeleksi matriks S dari $C_{t1, t2, t3.}$ Dalam hal ini m = 9, $s_1 = 4$, $s_2 = 5$ dan $s_T = 3$ seperti pada gambar 5 di atas. Angka dari pasangan subpixel menjadi

$$C_{\frac{9}{9},\frac{5}{9}}^{\frac{4}{9},\frac{5}{9}} = \left\{ \begin{matrix} \text{all permutations of} \\ \text{the columns of} \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} \right\}$$

IV. PERCOBAAN EVCS PADA GAMBAR *GRAYSCALE*

Pada bagian ini dilakukan percobaan enkripsi dan dekripsi EVCS pada gambar *grayscale*. Pertama-tama dilakukan pendefinisian gambar-gambar sebagai input gambar dan dipilih salah satu gambar sebagai *hidden image*, sedangkan gambar yang lain dijadikan *shadow image* atau gambar kamuflase.

Gambar 6. Gambar yang digunakan sebagai input enkripsi EVCS

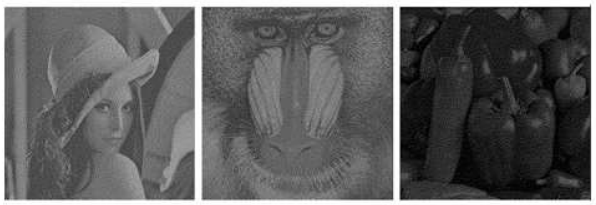
Gambar bertuliskan "hello world" paling kiri dianggap sebagai *hidden image* dan ketiga gambar di sebelah kanannya adalah *shadow images* atau gambar kamuflase.

Langkah berikutnya adalah mendefinisikan himpunan qualified dan forbidden. Pada kasus ini, himpunannya didefinisikan seperti di bawah ini:

$\tau_{Qual} = \{(1,2), (1,2,3)\}$

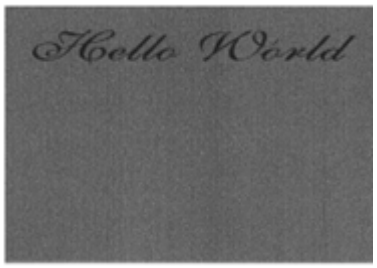
$\tau_{Forb} = \{(1), (2), (3), (1, 3), (2, 3)\}$

Kemudian dilakukan enkripsi *hidden image* sehingga didapatkan 3 buah *share* dengan gambar berikut.



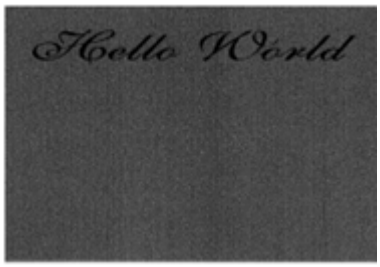
Gambar 7. Dari kiri ke kanan adalah gambar *share* 1, 2, dan 3

Ketika gambar 1 dan 2 ditumpuk, *hidden image* dapat diperoleh.



Gambar 8. *Hidden image* gabungan *share* 1 dan 2

Ketika gambar 1, 2 , dan 3 ditumpuk, *hidden image* juga dapat diperoleh dengan sedikit lebih jelas.



Gambar 9. *Hidden image* gabungan *share* 1, 2 dan 3

Ketika gambar 2 dan 3 ditumpuk, *hidden image* tidak muncul.

Gambar 10. Hasil gabungan *share* 2 dan 3 tidak menampilkan *hidden image*

Dapat kita lihat bahwa pada *Extended Visual Cryptography Schemes,* tiap *share* merupakan gambar yang bermakna. Secara kasat gambar *share* mata tidak jauh berbeda dengan gambar *shadow image* sebelum proses enkripsi sehingga sangat mengurangi kecurigaan pada pengamat, meskipun sebenarnya *image contrast* dan *pixel expansion* antara *shadow image* sebelum dan sesudah proses enkripsi terdapat perbedaan.

Dengan konsep *general access structure*, himpunan gambar yang terasosiasi pada *qualified* dapat memuncukan *hidden image*, sedangkan yang terasosiasi pada *forbidden* tidak dapat memunculkan *hidden image*.

V. PENERAPAN EVCS DALAM KEHIDUPAN

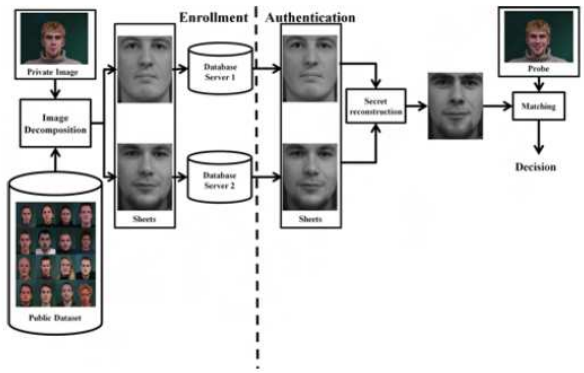
Dalam kriptografi visual, penerima *share* tidak memerlukan kunci atau komputasi untuk dekripsi, sehingga satu-satunya hal yang perlu diperhatikan adalah distribusi *share* sehingga aman dari pencurian *share* dan peningkatan kualitas *share* (gambar kamuflase) supaya mengurangi kecurigaan adanya kode rahasia pada *share* tersebut.

Dengan teknik EVCS, sebuah gambar dapat dienkripsi menjadi beberapa *share* yang memiliki makna sehingga menghindari kecurigaan pada orang yang melihat. Hal ini merupakan kelebihan utama EVCS dibandingkan teknik sebelumnya, yaitu VSSS. Karena keunggulan itulah EVCS diterapkan ke berbagai bidang pada kehidupan.

A. EVCS Untuk Autentifikasi Wajah Digital

Kerahasiaan data pribadi penduduk adalah hal yang sangat penting dan saat ini terdapat sistem autentifikasi menggunakan scan gambar wajah digital untuk memastikan apakah orang tersebut merupakan penduduk yang cocok seperti yang tersimpan pada basis data penduduk terpusat.

Skema autentifikasi wajah digital dapat menggunakan teknik EVCS untuk menjamin keamanan. Gambar di bawah ini merupakan skema dari pendekatan verifikasi wajah digital seorang penduduk [5]:



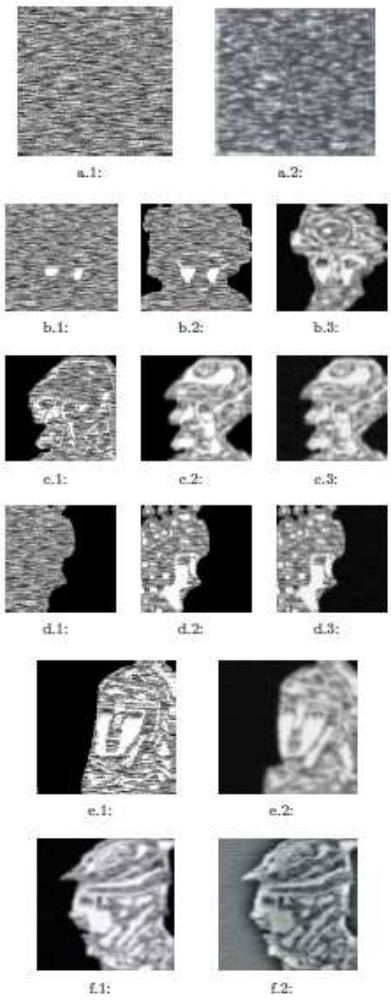
Gambar 11. Skema EVCS Pada Sistem Autentifikasi Wajah Digital

Bisa kita lihat bahwa pada skema di atas, pada saat pengambilan data (misalnya saat membuat KTP atau ID card) gambar original dienkripsi menggunakan komputasi kriptografi visual, kemudian *share* dari gambar tersebut dikamuflase dengan input foto-foto penduduk lain secara acak yang berasal dari basis data pusat. Kamuflase inilah yang merupakan ciri khas dari EVCS. Kemudian foto orisinil dapat dibangkitkan kembali dengan menggabungkan *share* kamuflase. Hasil penumpukan *share* dicocokkan dengan foto wajah digital saat melakukan autentifikasi.

B. EVCS Pada *Cocktail Party Effect*

Cocktail party effect adalah sebuah istilah kemampuan manusia untuk mengindentifikasi sebuah suara dari beberapa suara terutama ketika terdapat beberapa suara pengganggu (*noise*). Permasalahan utama *cocktail party effect* adalah bagaimana manusia dapat memilahkan suara manusia (*speech*), apa tanda-tanda manusia ketika melakukan pemilahan suara, dan apakah dapat dibuat sebuah mesin untuk melakukan hal yang serupa. Agustin mengemukakan bahwa penerapan EVCS pada pemecahan kode proses pada teknik biometrik (ilmu untuk mengemukakan identitas manusia berdasarkan fisik dan perilaku) dalam rangka memisahkan satu gambar dari yang lain dapat menjelaskan skema dari permasalahan ini [6].

Gambar di bawah ini merupakan contoh penerapan EVCS pada biometrik *cocktail party effect*.



C. Penyandian Dokumen Finansial

Prinsip EVCS juga dapat diaplikasikan pada transmisi dokumen konfidensial seperti dokumen keuangan dalam media internet. Contoh penerapan EVCS pada enkripsi dokumen finansial dilakukan oleh aplikasi VCRYPT yang diperkenalkan pertamakali oeh Hawkes et al. VCRYPT dapat mengodekan dokumen orisinil dengan skema (k,n) kemudian mengirim tiap-tiap *share*snya secara terpisah menggunakan email atau protokol FTP kepada resipien. Dekripsi kode hanya memerlukan operasi bit OR kepada seluruh *share*s dalam direktori tertentu dan tidak memerlukan komputasilainnya [7].

Para kriptanalis yang mencegat sebagian m dari n buah *share*s dimana m < k tidak dapat menampilkan dokumen orisinil yang disandikan. Bahkan, dengan teknik EVCS, kriptanalis bisa mendapatkan dokumen palsu yang menjadi kamuflase.

Dalam penerapan pada dokumen finansial, VCRYPT melakukan proses filterisasi setelah gambar asli berhasil didekripsi untuk meningkatkan kualitas digit. VCRYPT mengevaluasi m buah subpixel dan menampilkan pixel final sebagai hitam jika angka dari subpixel hitam melewati batas *threshold*.

D. Penyandian Suara Pada E-Voting

Mesin e-voting mengharuskan para pemilih untuk mempercayai integritas datanya. Chaum mengusulkan sistem e-voting berdasarkan (2, 2)-*threshold* VCS, yang menghasilkan olahan kuitansi enkripsi kepada setiap pemilih yang memungkinakan pelaksanaan verifikasi dalam menampilkan hasil voting. Di lokasi pemilihan, pemilih akan menerima kuitansi dua layer yang mencetak suara pemilihan, kemudian pemilih akan memberikan saah satu layer tersebut kepada panita pemilihan yang akan menghancurkan kertas tersebut. Layer satu lagi akan menjadi tak terbaca. Untuk memastikan suara pemilih tidak dihapus, pemilih dapat mengecek serial number pada kuitansi yang diperoleh setelah pemilihan dan melakukan "penumpukan" *share* yang dimiliki pemilih dan *share* yang didapatkan dari server yang mengakibatkan pemilih dapat melihat vote ia kembali [7].

Sistem ini memiliki beberapa kelebihan. Pertama, kuitansi yang tidak bisa digunakan untuk melakukan pengecekan vote dapat membuktikan bahwa terdapat gangguan/kecurangan pada sistem e-voting, dan kelebihan kedua adalah pemilih dapat teryakinkan bahwa vote yang terkirim ke server adalah sesuai dengan pilihannya.

VI. SIMPULAN

Dalam kriptografi visual, penerima *share* tidak memerlukan kunci atau komputasi untuk dekripsi, sehingga satu-satunya hal yang perlu diperhatikan adalah distribusi *share* sehingga aman dari pencurian *share* dan peningkatan kualitas *share* (gambar kamuflase) supaya mengurangi kecurigaan adanya kode rahasia pada *share* tersebut.

Dengan teknik EVCS, sebuah gambar dapat dienkripsi menjadi beberapa *share* yang memiliki makna sehingga menghindari kecurigaan pada orang yang melihat. Hal ini merupakan kelebihan utama EVCS dibandingkan teknik sebelumnya, yaitu VSSS. Karena keunggulan itulah EVCS diterapkan ke berbagai bidang pada kehidupan.

REFERENCES

[1] M. Naor and A. Shamir. (1995). *Visual Cryptography, Advances in Cryptology*. Eurocypt'94 Proceeding.

[2] G. Ateniese, C. Blndo, A. De Santis, and D. Stinson. (1996). *Visual Cryptography for General Access Structures*. Information and Computation.

[3] G. Atienese, C. Bundo, Alfredo De Santis, and Douglas R. Stinson. (2001). *Extended Capabilities for Visual Cryptography*. Theoritical Computer Science.

[4] N. Mizuho and Y.Yasushi. (2004). *Extended Visual Cryptography For Natural Images*. Department of Graphics and Computer Sciences Univ. Of Tokto.

[5] R.Arun and A. Asem. (2010). *Visual Cryptography for Face Privacy*. Lane Department of Computer Science and Electrical Engineering, West Virginia University, USA.

[6] Agustin, Nelly. (2011). *Extended Visual Cryptography Scheme with an Artificial Cocktail Party Effect*.

[7] Jim Cai. (2007). *A Short Survey on Visual Cryptography Schemes*.

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

Imam Prabowo K (13507123)