Analisis Perbandingan Berbagai Metode Dalam Kriptografi Visual

Edria Albert Varian W – NIM 13507031
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If17031@students.if.itb.ac.id

***Abstract*—Secret sharing merupakan metode untuk mendistribusikan suatu pesan rahasia pada suatu grup partisipan yang masing-masing akan mendapatkan satu bagian. Konsep secret sharing ini pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994 dan kemudian dikenal juga dengan instilah kriptografi visual. Pada intinya kriptografi visual menerapkan konsep kriptografi dalam menyembunyikan pesan kedalam suatu gambar tetapi dilakukan dengan suatu metode sehingga proses dekripsinya dapat dilakukan oleh pengelihatan manusia atau dapat dilakukan tanpa computer.**

Berbagai metode telah dikembangkan setelah konsep kriptografi visual ini diperkenalkan oleh Naor-Shamir pada jurnalnya "Visual Cryptography". Makalah ini akan membahas berberapa metode dari kriptografi visual yaitu Naor-Shamir Visual Sharing Scheme, Extended VSS – Gray Scale, Randomized VSS, Multi-pixel encoding method, dan General Access Structure beserta kelebihan dan kekurangan masing-masing metode.

***Index Terms*—Secret Sharing, Visual Cryptography, Visual Sharing Scheme, Naor-Shamir**

I. PENDAHULUAN

Kriptografi visual adalah salah satu teknik dalam kriptografi yang memungkinkan informasi yang bersifat visual untuk dienkripsi dengan metode tertentu dimana untuk mendekripsinya bisa dilakukan dengan pengelihatan manusia.

Kriptografi visual ini pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka mendemonstrasikan skema visual secret sharing. Secret sharing merupakan metode untuk mendistribusikan suatu pesan rahasia pada suatu grup partisipan yang masing-masing mendapatkan satu bagian. Secara lebih formal, skema secret sharing dapat diartikan terdiri dari satu pengirim dan n penerima. Pengirim akan memberikan pesan rahasia kepada penerima hanya jika kondisi tertentu telah dipenuhi. Pada secret sharing, setiap bagian harus minimal sama besar dengan pesan rahasia

Pada kriptografi visual sebuah gambar dipecah menjadi n-bagian yang disebut *share* sehingga jika seseorang memiliki n *share*, dia akan bisa mendekripsi gambar tersebut sedangkan n-1 *share* tidak akan memberikan informasi apa-apa mengenai gambar aslinya. Setiap *share* dicetak pada transparansi yang berbeda dan proses dekripsi dilakukan dengan menumpuk semua transparansi tersebut. Jika semua transparansi tersebut ditumpuk, maka gambar aslinya akan terlihat.

II. METODE PADA KRIPTOGRAFI VISUAL

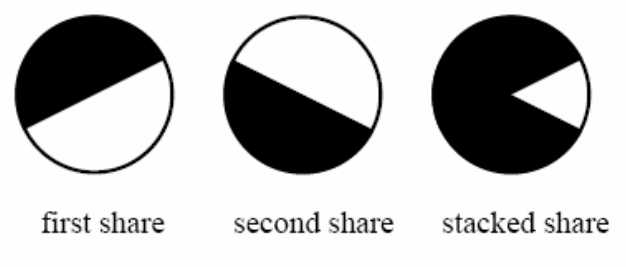
A. Naor-Shamir Visual Sharing Scheme

Pada metode yang diperkenalkan oleh Naor dan Shamir, setiap share merupakan kumpulan dari sebanyak *m* pixel hitam dan subpixel putih. Struktur datanya dapat direpresentasikan dengan matriks Boolean $n \times m$ $S = [s_{ij}]$ dimana s_{ij} bernilai 1 jika subpixel ke *j* pada transparansi ke *i* berwarna hitam. Saat akan menenkripsi pixel putih pada gambar rahasia, pertama kita secara random melakukan permutasi pada kolom M_0 lalu memilih baris ke *i* dari matriks yang telah dipermutasi untuk mengisi posisi yang berkorespondensi dengan *share* ke *i*. Setelah semua pixel pada gambar rahasia dienkripsi, *n share* akan terbentuk. Kemungkinan, setiap *share* akan memiliki ukuran *m* kali dari gambar aslinya, yang disebut *m pixel expansion*.

Untuk proses dekripsi, saat transparansi $i_1, i_2, \ldots, i_r$ disusun bersama, kita bisa melihat bahwa subpixel hitam direpresentaskan oleh array Boolean $i_1, i_2, \ldots, i_r$ pada S. Dari susunan ini dapat ditentukan suatu gray level yang sebanding dengan Hamming weight H(V) dari *m*-vector V yang telah dilakukan operasi OR. Gray level ini di interpretasikan oleh system visual sebagai warna hitam jika $H(V) \geq d$ dan diinterpretasikan sebagai warna putih jika $H(V) < d - \alpha m$ untuk rentan *threshold* $1 \leq d \leq m$ dan relative difference $\alpha > 0$.

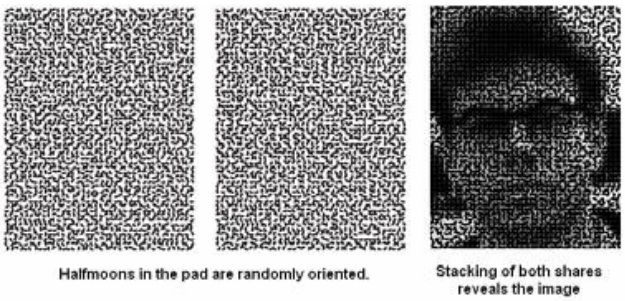
B.Extended VSS – Gray Scale

Naor dan Shamir menyebutkan bahwa banyak kemungkinan pengembangan dari dasar konsep yang mereka buat. Lebih jauh, mereka mengambangkan konsep yang mereka buat dengan menggunakan lingkaran yang terisi sebagian untuk merepresentasikan *grey values*, seperti yang dapat dilihat berikut:



Gambar1. Konsep stacked pada circle pixel

Gambar diatas menunjukan bahwa untuk tone yang kontinu pada *gray image* kita padat menggunakan pixel dengan bentuk bulat. Contohnya pada gambar berikut:



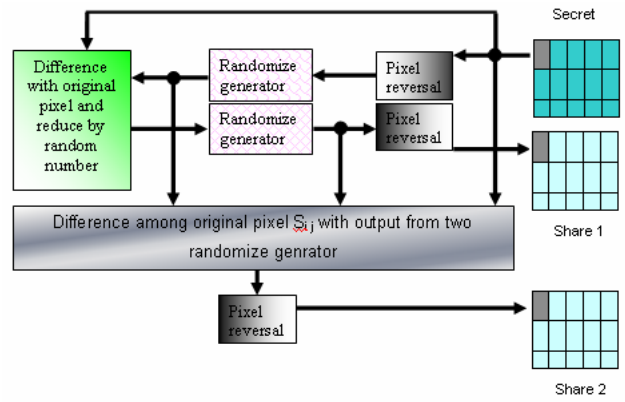
Gambar2. Hasil kriptografi visual dengan metode Extended VSS-Gray Scale

Untuk gambar yang dibagi menjadi lingkaran yang dirotasi seperti gambar diatas, kita bisa memberikan kesan warna dari abu-abu hingga hitam berdasarkan pengaturan dari superposisi.

C. Randomized VSS

Pada metode randomized VSS pendekatan yang dilakukan adalah randomization dan pixel reversal. Metode ini mengembangkan pendekatan pada VSS (2,2). Pada VSS (2,2) digunakan gambar *grayscale* (SI) sebagai input untuk algoritma. Dimana SI diasumsikan sebagai matriks S_{ij} dimana i dan j merupakan posisi pixel dan i,j = 1,2,3,…,n. Langkah-langkah pada metode ini adalah sebagai berikut:

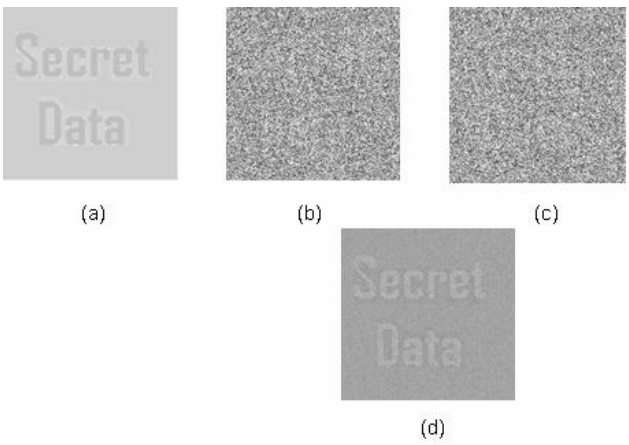
1. Pixel S_{ij} pada index i,j merupakan input yang disebut original pixel.
2. Lakukan pixel reversal misalnya $S_{ij}` = 255 - S_{ij}$
3. Gunakan generator angka random (0.1 hingga 0.9) untuk mengurangi $S_{ij}`$ secara random
4. Hitung perbedaan $S_{ij}`$ dengan pixel asli S_{ij}.
5. Gunakan generator angka random untuk mengurangi nilai dari $S_{ij}`$ yang telah direverse secara random
6. Lakukan pixel reversal misalnya $S_{ij}`` = 255 - S_{ij}`$
7. Simpan pada matriks sebagai gambar dengan nama share1.
8. Hitung perbedaan dari dua generator angka random dengan pixel asli S_{ij}.
9. Lakukan pixel reversal misalnya $S_{ij}``` = 255 - S_{ij}`$
10. Simpan $S_{ij}```$ pada matriks sebagai gambar dengan nama share2.
11. Ulangi langkah ke 1 hingga 10 untuk seluruh pixel pada matriks gambar sumber.



Gambar3. Skema metode Randomized VSS

Pada metode VSS biasanya gambar hasil dekripsi menjadi dua kali lebih besar dari pada gambar aslinya karena pixel p diekspansi menjadi dua subpixel. Dampak ini disebut pixel expansion yang akan mempengaruhi tingkat kekontrasan dari gambar hasil nantinya. Pada metode ini tidak ditemukan efek pixel expansion tetapi seperti metode VSS, pada metode ini gambar akhir yang dihasilkan terlihat lebih gelap dan terjadi beberapa kerusakan.

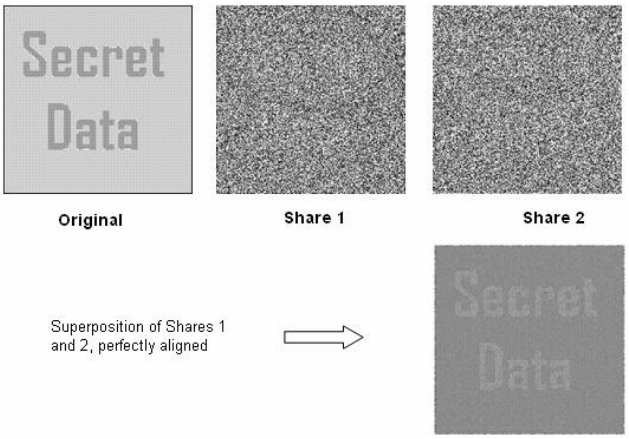
Metode ini tidak cocok untuk digunakan pada gambar yang gelap dengan tingkat kontas yang tinggi karena akan menghasilkan gambar yang semakin gelap dan menjadikan informasinya tidak dapat dibaca. Sedangkan pada testing menggunakan gambar yang berwarna terang dan memiliki tingkat kontras yang rendah, algoritma ini bisa menghasilkan gambar akhir yang dapat dilihat informasinya seperti pada gambar berikut:



Gambar4. Proses penerapan metode Randomized VSS

Penanganan kelemahan ini dapat dilakukan dengan menambahkan elemen preprocessing untuk mengubah gambar yang gelap atau memiliki kontras yang tinggi menjadi gambar *halftone*. Langkah ini dapat dilakukan sebelum gambar dipakai menjadi input algoritma randomized VSS ini. Tahap preprosesing tersebut dilakukan dengan menginisiasi nilai dari setiap pixel menjadi putih (255). Preprosesing ini mengubah tingkat

kontras gambar asli menjadi lebih rendah. Contoh pengaplikasian algoritma randomized VSS yang telah menggunakan preprosesing bisa dilihat pada gambar berikut:



Gambar5. Proses penerapan metode Randomized VSS dengan preprosessing

D. Multi-pixel Enncoding Methods

Seluruh metode yang dijelaskan sebelumnya menggunakan metode single-pixel encoding dimana algoritmanya melakukan enkripsi perpixel pada gambar awal. Dan ternyata effisiensi algoritmanya sangatlah rendah. Pada tahun 2004, Hou et al mengusulkan suatu metode multi pixel encoding dimana dalam satu loop akan menenkripsi *m* pixel, *m* adalah pixel expansion dan sebanding dengan jumlah kolom pada matriks basis. Walaupun metode ini memberikan peningkatan dalam effisiensi encoding, tetapi skema ini menghasilkan kualitas gambar akhir yang buruk jika dibandingkan dengan metode-metode lainnya. Lalu mereka mngajukan metode multi pixel encoding yang lain yang bisa meningkatkan kualitas dari gambar akhir. Skema yang baru ini juga mengencode *m* pixel dalam setiap loop walaupun *m* pixel tersebut dalam tipe yang sama.

Pada sisi yang lain, metode baru ini memiliki kekurangan karena kurang dari *m* pixel yang sama dan berurutan pada rantai input menyebabkan encoder akan melakukan trace backward atau forward untuk mengumpulkan *m* pixel dengan tipe yang sama untuk sekali run dan lebih dari *m* pixel sama yang berurutan mengakibatkan beberapa bagian yang redundan harus disimpan untuk loop berikutnya.

Fitur umum dari skema multi-pixel encoding adalah panjang pixel yang diencode bernilai constan *m*. Tetapi pada kenyataannya parameter *m* adalah pixel expansion dan karena itu biasanya nilai dari *m* biasanya dibatasi pada range yang sangat kecil, yang mengakibatkan peningkatan dalam effisiensi encodingnya menjadi tidak terasa. Pada sisi lain, faktanya pada aplikasi jumlah dari consecutive pixel yang memiliki tipe yang sama pada suatu gambar akan lebih besar daripada nilai *m*. Ini berarti nilai tetap dari *m* tidak cocok untuk kasus input sebenarnya.

E. General Access Structure

Sebenarnya, struktur akses merupakan suatu aturan yang mendefinisikan pembagian gambar rahasia. Contoh yang paling umum adalah struktur akses threshold (n,n) dan (t,n). Pada struktur akses threshold (t,n) mengatur bahwa sebanyak *t* atau hingga *n* partisipan dapat berkerja sama untuk mengungkap gambar rahasia dan apabila terdapat kurang dari *t* partisipan maka mereka tidak akan mendapatkan apa-apa. Sebenarnya, struktur akses threshold (n,n) adalah sebuah contoh dari (t,n). Struktur ini membutuhkan semua partisipan untuk bekerja sama untuk mendapatkan makna dari gambar rahasia dan tidak akan mendapat apa-apa jika salah satu tidak ada. Jadi (t,n) dapat dikatakan lebih toleran karena makna rahasianya masih dapat diungkap oleh *t* share walaupun (n-t) share sisanya korup.

Struktur akses threshold hanya sebuah kasus special yang disebut general access structure. Biasanya general access structure dinotasikan sebagai $\wp = \{A_0, A_1\}$ dimana A_0 dan A_1 adalah set subset dari semua partisipan dan $A_0 \cap A_1 = \emptyset$. A_0 merepresentasikan sekumpulan set yang terlarang dan A_1 meprepresentasikan sekumpulan set yang memenuhi kualifikasi. Jika kita menumpuk seluruh share yang memenuhi kualifikasi maka akan dapat memunculkan gambar rahasia, tetapi menumpuk share yang dimiliki oleh partisipan dari set terlarang yang manapun tidak bisa untuk memunculkan informasi apa-apa mengenai gambar rahasia. Contohnya pada suatu system yang terdiri dari 4 partisipan, kita membuat A_1 = {{1, 2}, {2, 3}, {3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2, 3, 4}}, yang menyebabkan A_0 = {{1}, {2}, {3}, {4}, {1, 3}, {1, 4}, {2, 4}}. Dari sini kita dapat melihat bahwa menumpuk share1 dan share 2 akan dapat memunculkan gambar rahasia sedangkan menumpuk share1 dan share 4 tidak dapat mendapatkan apa-apa mengenai gambar rahasia.

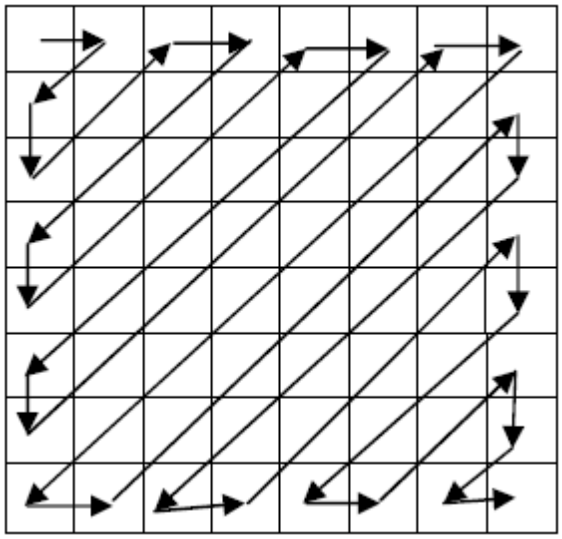
General access structure akan mengikuti property monotone, jika $\gamma \in A_1$ dan $\gamma \subseteq \gamma`$, maka $\gamma \in A_1$; jika $\lambda \in A_0$ dan $\lambda \supseteq \lambda`$ maka $\lambda` \in A_0$. Jadi kita dapat melihat bahwa {1,2} $\in A_1$ yang berakibat bahwa {1, 2, 3} $\in A_1$, {1, 2, 4} $\in A_1$, {1, 2, 3, 4} $\in A_1$; dan {1, 4} $\in A_0$ menyebabkan {1} $\in A_0$ dan {4} $\in A_0$. Lebih jauh lagi, kita dapat mengatakan bahwa $A_1^- = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ dan $A_1^+ = \{\{1, 3\}, \{1, 4\}, \{2, 4\}\}$ untuk menampilkan nilai A_1 dan A_0 secara berturut turut pada property monotone.

F. Pixel-block Aware Encoding

Secara umum, metode ini menggunakan matriks M_0 dan M_1 untuk mengencode pixel putih dan hitam, dan memiliki dimensi yang sama *n x m*. Gambar rahasia yang akan diencode adalah SI dengan ukuran L x H pixel dan sejumlah *n* share $\{S_0, S_1,\ldots,S_n\}$. Pada gray-scale atau kromatik image, pixel putih biasanya berarti blank dan pixel hitam berarti non-blank.

a) Scanning Mode
   Selama proses enkripsi dari gambar rahasia, encoder perlu untuk memindai satu atau lebih pixel, dan biasanya pemindaian dilakukan baris-perbaris. Pada

metode ini pemindaian dilakukan secara zigzag untuk meningkatkan adaptability. Skema pemindaian dapat dilihat sebagai berikut:



Gambar6. Zigzag scanning order

b) Encoding

Sama seperti skema Naor-Shamir, skema yang dipakai juga memiliki dua tahap, distribusi dan rekontruksi. Pada fase rekontruksi metode ini akan menumpuk share yang benar sehingga dapat memunculkan informasi yang tersembunyi.

INPUT: *SI* with $L \times H$ pixels; M_0 and M_1 with size of $n \times m$, respectively.
OUTPUT: $S_1, S_2, \ldots, S_n$ with $L \times H$ pixels, respectively.
step1: scan the secret image *SI* using zigzag mode till meeting different pixel or reaching the end of *SI*, and then two values are known: *r*, the span of this run, and *p*, the pixel type. There is $p = 0$ for white pixel, otherwise $p = 1$.
step2: $\boldsymbol{L} = \emptyset$;
step3: while ($|\boldsymbol{L}| < r$)
{
step3.1: randomly rearrange (1, 2, …, *m*) and write the result as ($l_1, l_2, \ldots, l_m$);
step3.2: $\boldsymbol{L} = \boldsymbol{L} \,||\, (l_1, l_2, \ldots, l_m)$; /* "||" means vector concatenation operation */
}
step4: if ($|\boldsymbol{L}| > r$)
{
step4.1: truncate the tail of $\boldsymbol{L}$ to make sure that $|\boldsymbol{L}| = r$;
}
step5: fill the pixels at line *i* and the columns indicated by $\boldsymbol{L}$ of M_p into S_i, where $i = 1, 2, \ldots, n$, using the same mode during scanning.
step6: if scanning does not reach the end of *SI*, go to *step1*; otherwise terminate.

Gambar7. Algoritma pixel-block aware encoding

c) Security

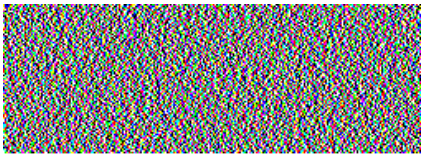
Tingkat keamanan metode ini sebanding dengan tingkat keamanan metode Naor-Shamir, dan keamanan metode Naor-Shamir masih dinilai baik.

d) Complexity

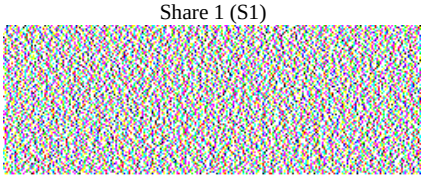
Dibandingkan dengan metode multi-pixel encoding yang lain, kompleksitas metode ini bisa dibilang sebanding atau bahkan lebih rendah. Metode ini menyimpan lebih sedikit variable dalam perpindahaan loopnya.

Dalam pengembangannya, metode ini juga sudah dikembangkan untuk dapat melakukan enkripsi pada gambar berwarna walaupun hasil akhir yang didapat masih mengandung banyak noise.

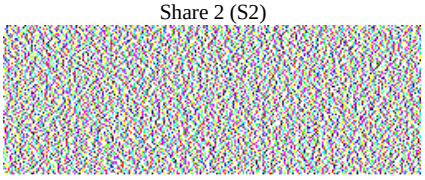
Berikut merupakan proses stacking pada enkripsi gambar berwarna:



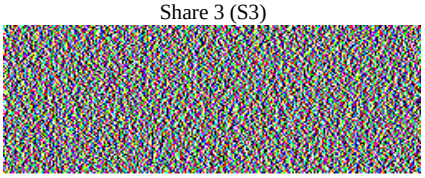
Share 1 (S1)



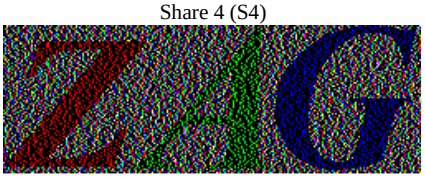
Share 2 (S2)



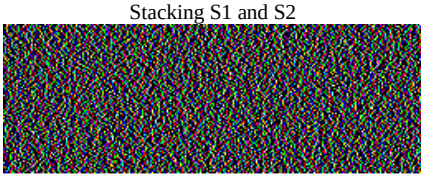
Share 3 (S3)



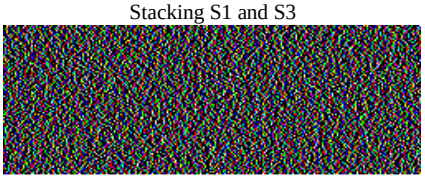
Share 4 (S4)



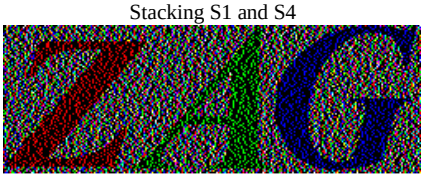
Stacking S1 and S2



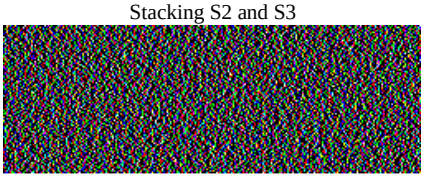
Stacking S1 and S3



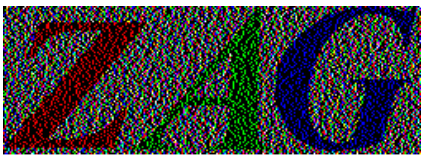
Stacking S1 and S4



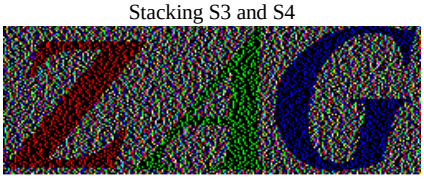
Stacking S2 and S3



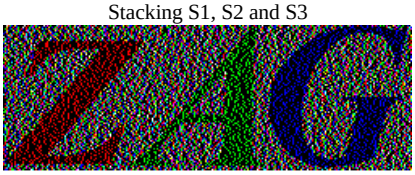
Stacking S2 and S4



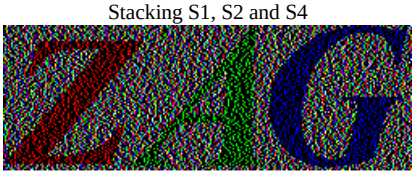
Stacking S3 and S4



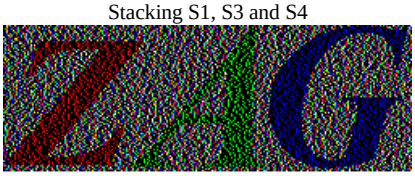
Stacking S1, S2 and S3



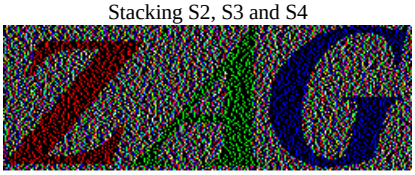
Stacking S1, S2 and S4



Stacking S1, S3 and S4



Stacking S2, S3 and S4



Stacking S1, S2, S3 and S4

V. KESIMPULAN

Konsep kriptografi visual yang diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994 telah mengalami banyak perkembangan. Setelah konsep tersebut diperkenalkan, banyak bermunculan metode baru dalam kriptografi visual. Dari metode-metode tersebut ada yang melakukan improvisasi pada metode visual sharing scheme yang dibuat oleh Naor-Shamir seperti pada metode Extended VSS-Gray Scale, Randomized VSS maupun metode baru yang mencoba menawarkan cara baru dalam melakukan encoding seperti Multi-pixel encoding ataupun metode yang membatasi pembagian sharenya yaitu General Access Structure.

Dari kelima metode yang dibahas tentunya masing-masing memiliki kelebihan dan kekurangan masing-masing. Untuk metode VSS yang diperkenalkan oleh Naor-Shamir, metode ini memiliki kelebihan dalam hal simplicity jika dibandingkan dengan metode-metode lain. Dan karena metode ini yang pertama kali diperkenalkan sehingga metode ini menjadi dasar untuk pengembangan berbagai metode lainnya. Kelemahan metode VSS Naor-Shamir adalah algoritmanya yang dinilai kurang effisien dalam proses encoding. Dan juga dukungan terhadap berbagai intensitas tone yang masing kurang. Pada Extended VSS-Gray Scale, metode ini berusaha menutupi kekurangan VSS sebelumnya dengan menambahkan fitur circle pixel, sehingga gambar akhir yang dihasilkan dapat memiliki tone yang lebih beragam. Kelemahan dari metode ini masih terletak pada proses enkripsinya yang melakukan proses per pixel dan dinilai kurang efektif.

Metode ketiga adalah Randomized VSS. Metode ini memiliki keunggulan dalam hal keamanan data pada tahap share. Dengan adanya mekanisme random pada saat pembangkitan share maka data pada tahap share akan lebih sulit untuk diinterpretasikan tanpa gabungan dari share-share yang lain. Kekurangan metode ini ada pada dukungan gambar yang memiliki kontras yang tinggi, dimana pada gambar sumber yang memiliki kontras yang tinggi akan menghasilkan gambar akhir yang gelap dan memiliki tingkat noise yang tinggi dan ada kemungkinan tidak dapat terbaca. Masalah ini bisa dikurangi dengan melakukan preprosesing pada gambar sebelum menjadi input untuk metode ini, tetapi hasilnya ternyata kurang signifikan.

Metode keempat adalah Multi-pixel encoding. Metode ini berusaha menutupi kelemahan VSS pada sisi efisiensi algoritma, tetapi nyatanya kurang cocok untuk diterapkan pada dunia nyata. Metode ini malah menimbulkan beberapa kekurangan baru yaitu pertama kualitas gambar akhir yang dihasilkan masih buruk sehingga terdapat kemungkinan hasil akhir tidak dapat dibaca. Yang kedua terdapat ketidak-efisienan dalam hal penggunaan resource computer dimana setiap loop perhitungan membutuhkan resource lebih untuk menyimpan hasil dari perhitungan sebelumnya. Dan juga yang paling fatal adalah ketidak sinkronan nilai *m* antara algoritma dan dunia nyata sehingga tingkat eror nya cukup tinggi saat diimplementasikan.

Metode kelima adalah General Access Structure, metode ini sedikit berbeda dengan metode lainnya dimana metode ini mengatur aturan distribusi dari share bukan mendefiniskan algoritma enkripsi seperti metode-metode lain yang sudah dibahas. Kelebihan metode ini adalah, metode ini dapat digabungkan dengan metode-metode enkripsi yang lain sehingga meningkatkan tingkat keamanan dari metode kriptografi visual. Dan juga dengan metode ini kita bisa memberikan hak akses tertentu pada setiap kelompok partisipan.

REFERENCES

Mousa. Talal, Khalid. Aleem, *New Algorithm for Halftone Image Visual Cryptography*, Dhahran, Saudi Arabia, King Fahd University of Pet. & Min.

Naor, M. and Shamir, A., Visual cryptography, *In Proc.Eurocrypt 94*, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag., 1994, 1–12.

http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html *Doug Stinson's Visual Crytography Page*. University of Waterloo

Zhang. Haibo, *Visual Cryptography for General Access Structure Using Pixel-block aware Encoding*. Wuhan Digital Engineering Institute, China. http://www.academypublisher.com/jcp/vol03/no12/jcp03126875.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, 29 April 2010

ttd

Edria Albert Varian W
13507031