Perbandingan Metode *Visual Sharing Scheme* dan *General Access Structure* pada Kriptografi Visual

Shofi Nur Fathiya - 13508084
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18084@students.if.itb.ac.id

***Abstract*—Salah satu teknik yang digunakan untuk menjaga kerahasiaan citra pada ilmu kriptografi adalah kriptografi visual. Kriptografi ini menggunakan konsep secret sharing, yaitu membagi suatu citra menjadi beberapa bagian kemudian mendistribusikan bagian dari citra tersebut ke beberapa orang dalam suatu grup. Untuk mendapatkan citra yang utuh kembali, beberapa atau semua bagian tersebut harus disatukan. Bagian dari citra tersebut dikenal dengan nama share.**

Metode yang digunakan dalam kriptografi visual bermacam-macam, mulai dari yang paling sederhana hingga yang cukup kompleks. Pada makalah ini, akan dibahas dua metode dengan teknik yang dianggap cukup berbeda, yaitu Visual Sharing Scheme dan General Access Structure untuk kemudian dibandingkan. Visual Sharing Scheme merupakan metode pertama yang diciptakan dalam kriptografi visual dan menjadi dasar bagi metode-metode lainnya, salah satunya General Access Structure. Kedua metode ini masing-masing memiliki kelebihan dan kekurangan dalam menjaga kerahasiaan citra.

***Index Terms*—citra, share, kriptografi visual, Visual Sharing Scheme, General Access Structure.**

I. PENDAHULUAN

Kriptografi merupakan ilmu yang mempelajari mengenai bagaimana cara menyembunyikan sebuah pesan agar tidak mudah diketahui oleh pihak yang tidak berkepentingan. Kriptografi banyak diaplikasikan di berbagai media, terutama media digital. Tidak hanya pesan teks biasa, kriptografi juga dapat digunakan untuk menjaga kerahasiaan pesan berupa citra.

Salah satu metode yang seringkali digunakan untuk menyembunyikan pesan berbentuk citra adalah kriptografi visual. Kriptografi visual adalah suatu teknik menyembunyikan informasi citra dengan cara membaginya menjadi beberapa citra transparan atau yang biasa disebut sebagai share. Bila dilihat oleh mata biasa, masing-masing share ini tidak memiliki informasi apapun. Hanya sepotong gambar biasa yang bahkan seringkali tidak jelas apa bentuk atau gambarnya. Hal ini dimaksudkan untuk menghilangkan kecurigaan pada orang lain, sehingga informasi pada citra hanya dapat diketahui oleh orang-orang yang memiliki share saja.

Untuk mendapatkan citra kembali seperti semula, share-share yang ada cukup ditumpuk begitu saja. Ini merupakan salah satu keunggulan kriptografi visual, dimana dalam melakukan dekripsi tidak diperlukan algoritma yang rumit ataupun kunci sama sekali sehingga citra asli dapat dengan mudah didapatkan asalkan share dimiliki.

Kriptografi visual pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka membuat sebuah makalah yang berisi cara baru dalam menyembunyikan pesan gambar. Cara yang mereka gunakan ini sangat sederhana, namun seiring dengan perkembangan teknologi, banyak orang menciptakan cara-cara baru yang lebih kompleks dalam kriptografi visual. Pada makalah ini akan dibahas dua metode, yaitu *Visual Sharing Scheme*, yang merupakan metode paling sederhana, dan metode *General Access Structure*, yang merupakan pengembangan dari metode *Visual Sharing Scheme*. Citra yang dibahas pada kedua metode ini terbatas hanya pada citra hitam putih saja.

II. DASAR TEORI

A. Visual Sharing Scheme

Visual Sharing Scheme (*Secret Sharing Scheme*) merupakan 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 informasi mengenai citra.

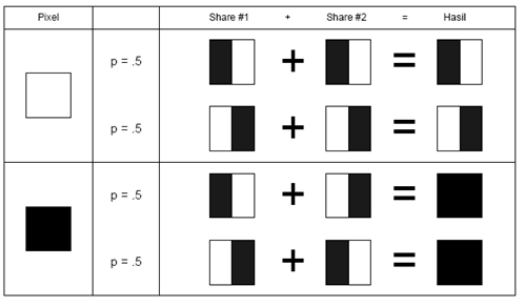
Share pertama pada *Visual Sharing Scheme* didapatkan dari nilai random masing-masing pixel. Untuk gambar hitam putih, nilai random hanya berkisar antara dua nilai, yaitu hitam atau putih untuk setiap pixelnya. Hasil dari citra random ini adalah citra dengan warna hitam-putih yang tak beraturan. Setelah 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.

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.

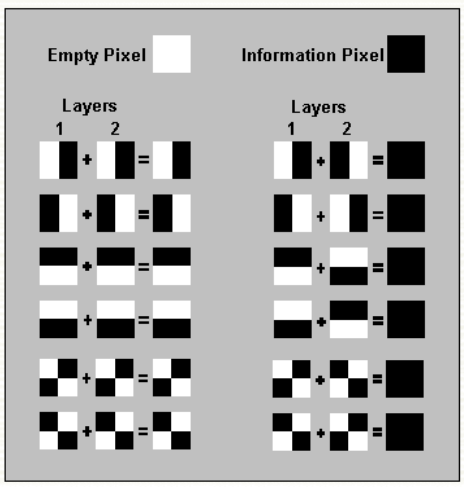
Contoh sederhana dari pembagian subpixel ini adalah dengan membagi tiap pixel menjadi 2 subpixel seperti gambar di bawah ini.



Gambar 1. Model kriptografi visual untuk 2 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.

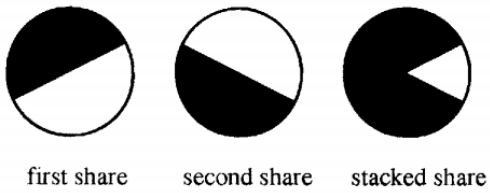
Contoh lainnya adalah dengan membagi satu pixel menjadi 4 subpixel dengan 2 subpixel berwarna hitam dan 2 subpixel lainnya berwarna putih untuk setiap pixelnya. Model 4 subpixel beserta kemungkinan susunannya adalah sebagai berikut.



Gambar 2. Model kriptografi visual untuk 4 subpixel

Untuk pembagian dengan 4 subpixel, terdapat 6 kemungkinan pasangan untuk 2 share. Sama seperti 2 subpixel, pada 4 subpixel pun warna pixel yang dihasilkan akan berwarna hitam bila subpixel pada kedua shre berbeda dan berwarna putih jika sama.

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



Gambar 3. Model kriptografi visual dengan lingkaran

B. General Access Structure

Metode ini merupakan pengembangan dari metode *Visual Sharing Scheme*. Perbedaan yang mencolok antara kedua metode ini terletak pada jumlah share dan fungsi dari share tersebut. Jumlah share pada *General Access Structure* dapat lebih dari 2, misalnya 3, 4, atau 5. Selain itu, 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.

Beberapa hal yang perlu diingat mengenai General Access Structure adalah sebagai berikut.

1. Set partisipan : P = {1,2,…..,n}
2. Qualified set (G_{qual}), yaitu kumpulan beberapa share yang bila digabungkan dapat membentuk citra asal. $G_{qual} \subset 2P$.
3. Forbidden set (G_{forb}), yaitu kumpulan beberapa share yang bila digabungkan tidak akan

membentuk citra asal. $G_{forb} \subset 2P$.

4. Jika $G_{qual} \cap G_{forb} = 0$ maka (G_{qual}, G_{forb}) merupaka *General Access Structure Scheme*.

Jumlah share pada G_{qual} tidak selalu sama. Matriks solusi yang digunakan pun dapat bermacam-macam. Misalnya saja, untuk P = {1,2,3,4}, G_{qual} = {{1,4}, {1,2,3}} dan matriks S_0 (matriks untuk warna putih) dan matriks S_1 (matriks untuk warna hitam) adalah sebagai berikut.

$$S^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Gambar 4. Matriks S_0 dan S_1

Pada metode ini, penumpukan share dapat dianggap sebagai fungsi OR, dimana ada satu saja share yang pixelnya hitam, maka pixel yang dihasilkan juga akan berwarna hitam. Pixel putih tidak dapat menghapuskan pixel hitam, namun sebaliknya, pixel hitam dapat menghapuskan pixel putih. Tingkat keabu-abuan yang dihasilkan dari penumpukan ini dapat dianggap sebagai warna hitam ataupun putih, bergantung dari nilai Hamming Weight atau H(V) dari pixel tersebut. Pixel dinyatakan sebagai hitam ketika nilai $H(V) \geq d$ dan pixel dinyatakan sebagai putih ketika nilai $H(V) \leq d-\alpha.m$.

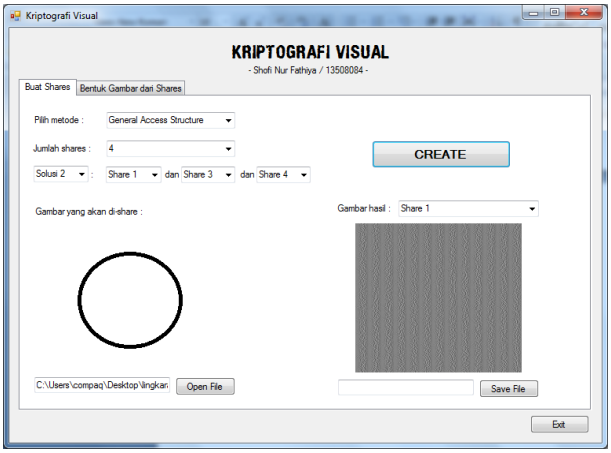
Adapun beberapa parameter penting terkain kriptografi visual ini adalah sebagai berikut.

1. m, menyatakan jumlah subpixel pada share. Parameter ini menentukan seberapa besar resolusi hilang dari citra sehingga parameter m diusahakan bernilai sekecil mungkin.
2. α, menyatakan perbedaan relatif nilai H(V) hasil penumpukan pixel putih dan hitam pada share. Parameter ini merepresentasikan besarnya kontras sehingga diusahakan bernilai sebesar mungkin.
3. r, merupakan besarnya kumpulan matriks C_0 dan C_1. C_0 merupakan kumpulan matriks untuk pixel warna putih dan C_1 merupakan kumpulan matriks untuk pixel warna hitam. Besarnya C_0 dan C_1 ini tidak harus sama, namun biasanya dianggap sama, yaitu jumlah permutasi kolom yang mungkin untuk setiap matriks dalam C_0 dan C_1 adalah m!.

III. PENGUJIAN PROGRAM

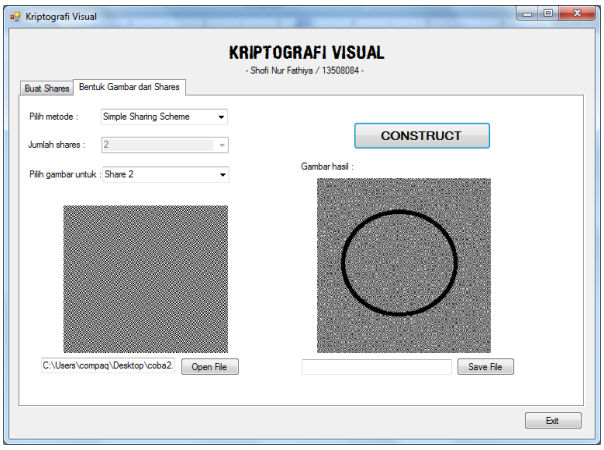
Program yang dibuat menguji perbedaan antara *Visual Sharing Scheme* dan *General Access Structure*. Citra yang diujikan pada program ini terbatas pada citra hitam-putih saja.

Tampilan utama program untuk proses pembuatan share dari citra asal adalah sebagai berikut.



Gambar 5. Tampilan program untuk pembuatan share dari citra asal

Sedangkan tampilan utama untuk proses konstruksi citra dari share adalah sebagai berikut



Gambar 6. Tampilan program untuk konstuksi citra asal dari share

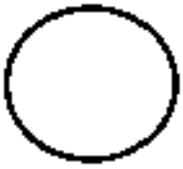
A. Pengujian *Visual Sharing Scheme*

Pada pengujian ini, setiap pixel akan diubah menjadi 4 subpixel dengan definisi masing-masing pixel adalah sebagai berikut.

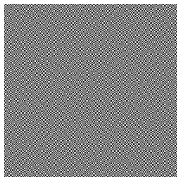
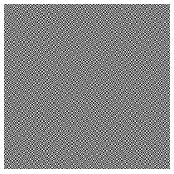
(a) (b)

Gambar 7. Representasi subpixel untuk pixel berwarna (a) putih dan (b) hitam

Citra yang akan dipecah menjadi 2 buah share adalah citra lingkaran.bmp. Untuk membentuk kembali citra asal, kedua share diperlukan dalam proses konstruksi. Berikut merupakan citra asal dan hasil sharenya.



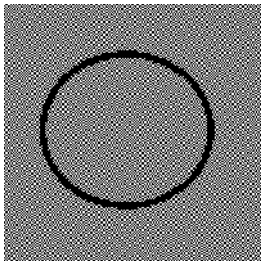
Gambar 8. File lingkaran.bmp

Share 1 Share 2

Gambar 9. Hasil share

Untuk mendapatkan kembali citra asal, kedua share harus ditumpuk. Hasilnya adalah sebagai berikut.



Gambar 10. Hasil penggabungan share 1 dan share 2 pada metode Visual Sharing Scheme

Citra yang dihasilkan memang tidak sama persis dengan citra aslinya karena terdapat banyak noise yang dihasilkan saat proses konstruksi. Namun, dapat terlihat bahwa informasi pada citra asal dan citra hasil konstuksi ini sama.

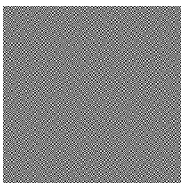
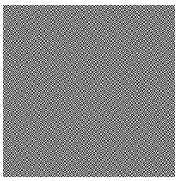
B. Pengujian *General Access Structure*

Pengujian metode General Access Structure menggunakan citra yang sama dengan metode sebelumnya, yaitu lingkaran.bmp. Solusi yang dihasilkan untuk metode ini adalah :

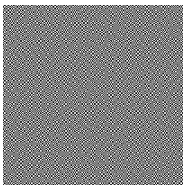
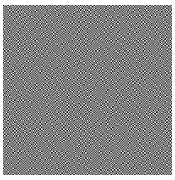
- P = {1,2,3,4}
- Gqual = {{1,2}, {1,3,4}}

Dengan kata lain, jumlah share yang dihasilkan dari metode ini berjumlah 4 share, dan untuk membentuk citra asli terdapat dua cara, yaitu dengan menggabungkan share 1 dan share 2 atau menggabungkan share 1, share 3, dan share 4. Penggabungan di luar itu tidak akan menghasilkan citra asal.

Hasil share yang didapat dari metode ini adalah sebagai berikut.

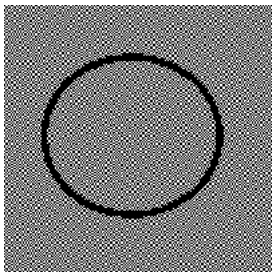
Share 1 Share 2

Share 3 Share 4

Gambar 11. Hasil share dengan metode *General Access Structure* dengan jumlah share = 4.

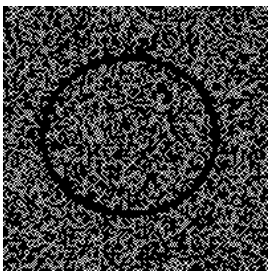
Selanjutnya adalah menggabungkan share untuk mendapatkan kembali citra. Cara pertama adalah dengan menggabungkan share 1 dan share 2. Hasilnya adalah sebagai berikut.



Gambar 12. Penggabungan share 1 dan share 2 pada metode *General Access Structure*

Hasil yang didapat tidak berbeda jauh dengan penggabungan 2 share pada metode *Visual Sharing Scheme*.

Cara kedua adalah dengan menggabungkan 3 buah share, yaitu share 1, share 3, dan share 4. Hasil yang didapat adalah sebagai berikut.



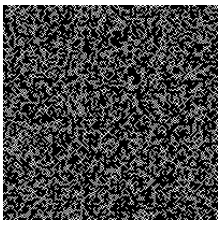
Gambar 13. Penggabungan share 1, share 3, dan share 4 pada metode *General Access Structure*

Terlihat bahwa ketika menggabungkan 3 buah share, gambar yang dihasilkan memiliki lebih banyak noise dibandingkan dengan hanya menggabungkan 2 share saja.

Untuk membuktikan bahwa penggabungan share lainnya tidak memiliki informasi, maka dilakukan

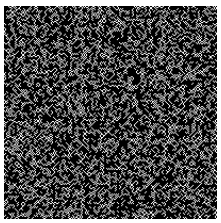
pengujian dengan menggabungkan share yang tidak termasuk pada Gqual. Hasil yang didapat dari beberapa pengujian Gforb adalah sebagai berikut.

- Share 1 + Share 3



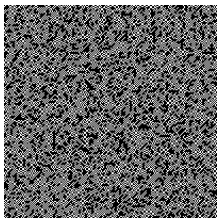
Gambar 14. Penggabungan share 1 dan share 3

- Share 2 + Share 3



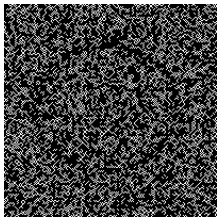
Gambar 15. Penggabungan share 2 dan share 3

- Share 2 + Share 4



Gambar 16. Penggabungan share 2 dan share 4

- Share 2 + Share 3 + Share 4



Gambar 17. Penggabungan share 2, share 3, dan share 4

Pada hasil penggabungan share 2 + share 3 + share 4, gambar lingkaran hampir terlihat. Ini dikarenakan dari 3 share yang digabungkan, 2 diantaranya yaitu share 3 dan share 4 merupakan bagian dari solusi kedua, yaitu share 1 + share 3 + share 4.

IV. ANALISIS DAN PEMBAHASAN

Pada metode Visual Sharing Scheme, cara yang digunakan cukup sederhana, hanya dengan membagi citra menjadi 2 buah share. Share pertama didapatkan dengan random, sedangkan share lainnya didapat dengan memperhitungkan share pertama dan citra asli.

Terlihat bahwa citra hasil penggabungan memiliki noise yang tidak terlalu banyak sehingga informasi pada citra dapat dengan mudah terlihat. Jumlah share yang diperlukan untuk mendapatkan kembali citra pun tidak banyak, cukup 2 share saja. Metode ini cocok untuk digunakan ketika informasi hanya ingin dishare hanya untuk 2 orang saja. Namun karena hanya ada satu cara untuk mendapatkan kembali informasi pada citra, akan menjadi masalah ketika salah satu share hilang atau rusak. Jika salah satu share tidak dapat lagi digunakan, maka informasi pada citra menjadi tidak bisa didapatkan kembali.

Pada metode *General Access Structure*, cara yang digunakan dalam membentuk share-share yang ingin dihasilkan tidak sesederhana pada metode *Visual Sharing Scheme*, terutama ketika solusi yang diinginkan terdiri dari 3 atau lebih share. Contohnya seperti yang diujikan pada program, dimana citra dibagi menjadi 4 share dan untuk membentuk kembali citra diperlukan share 1 + share 2 atau share 1 + share 3 + share 4. Share 1 dapat dibentuk dengan mudah, yaitu dengan fungsi random. Share 2 dapat dibentuk dengan memperhitungkan share 1 dan citra asal. Cara ini sama dengan cara pada *Visual Sharing Scheme*. Namun pembentukan share selanjutnya tidak semudah pembentukan share 1 dan share 2. Pada pembuatan program, share 3 didapat dari hasil random, sama seperti share 1. Namun saat pembentukan share 4, share 1 dan share 3 harus ikut diperhitungkan. Tentu hal ini lebih rumit dibandingkan ketika hanya memperhitungkan 1 share saja. Semakin banyak share yang diperlukan, semakin rumit mendapatkannya.

Banyaknya share juga ternyata mempengaruhi faktor lain, yaitu noise. Noise yang dihasilkan ketika menggabungkan 3 buah share lebih banyak daripada menggabungkan 2 buah share saja. Hal ini dikarenakan pixel putih hanya terbentuk ketika seluruh pixel pada share berwarna putih. Terdapat satu saja pixel pada share yang berwarna hitam, maka pixel yang dihasilkan pun akan berwarna hitam. Pada penggabungan 2 buah share, kemungkinan seluruh pixel pada share berwarna putih lebih besar dibandingkan dengan kemungkinan seluruh pixel pada share berwarna putih pada penggabungan 3 buah share. Sebaliknya, pixel hitam lebih besar kemungkinannya untuk terbentuk pada penggabungan 3 buah share daripada penggabungan 2 buah share. Pixel hitam inilah yang menyebabkan banyaknya noise yang dihasilkan saat penggabungan share selesai dilakukan. Semakin banyak share yang digabungkan, noise yang dihasilkan akan semakin banyak.

Metode *General Access Structure* juga memiliki kelebihan disamping kekurangan seperti yang telah

dijelaskan sebelumnya. Karena jumlah share pada metode ini bisa berapapun, tidak harus 2 share, maka share bisa dibagikan ke lebih banyak orang. Hal ini sangat berguna ketika jumlah orang yang ingin diberikan informasi cukup banyak, lebih dari 2 orang.

Kelebihan lainnya terletak pada pembagian solusi. Pada metode *General Access Structure*, set solusi dalam mendapatkan kembali informasi citra dapat berjumlah lebih dari satu. Hal ini akan sangat membantu pada kondisi tertentu, misalnya ketika tidak harus semua anggota grup yang memiliki share berkumpul untuk mendapatkan informasi citra asli. Cukup beberapa saja, misal orang 1 hanya bertemu dengan orang 2, orang 3 cukup bertemu dengan orang 4 dan orang 5, dan sebagainya. Banyaknya solusi set ini pun akan sangat berguna ketika terdapat salah satu share yang hilang. Misalkan ketika solusi yang diperlukan untuk membentuk citra asal adalah share 1 + share 2 dan share 1 + share 3 + share 4. Jika share 2 hilang, maka informasi masih bisa didapatkan melalui gabungan share 1 + share 3 + share 4. Begitu pula ketika share 3 atau share 4 menghilang, masih ada share 1 dan share 2 yang dapat membentuk citra asal.

Pada *General Access Structure* pun, kombinasi pada set solusi yang dihasilkan bisa dipilih sendiri. Hal ini dapat memudahkan dalam pembagian share ke anggota grup.

V. KESIMPULAN

Kesimpulan yang didapat dari analisis dan perbandingan kedua metode kriptografi visual ini adalah bahwa masing-masing metode memiliki kelebihan dan kekurangan sebagai berikut.

1. *Visual Sharing Scheme*
   Kelebihan :
   - Noise yang dihasilkan saat penggabungan share untuk mendapatkan kembali citra asal sedikit.

   Kekurangan :
   - Jika ada satu share yang hilang maka informasi pada citra tidak bisa didapatkan.
2. *General Access Structure*
   Kelebihan :
   - Ketika ada salah satu share yang hilang, ada kemungkinan bahwa informasi pada citra asal masih bisa didapatkan.

   Kekurangan :
   - Semakin banyak share yang digabungkan, semakin besar pula noise yang dihasilkan.

Penggunaan kedua metode ini berbeda tergantung kondisinya. Kondisi yang cocok untuk masing-masing metode adalah sebagai berikut.

1. *Visual Sharing Scheme*
   Ketika jumlah orang yang perlu diberi share hanya 2 orang dan share tidak mudah rusak ataupun hilang.
2. *General Access Structure*
   Ketika jumlah orang yang perlu diberi share cukup banyak, lebih dari 2 orang dan perlu backup sebagai antisipasi jika ada share yang hilang.

REFERENCES

[1] Romdhoni, Muhammad Arif.. “Kriptografi Visual pada Citra Biner dan Citra Berwarna Serta Pengembangannya dengan Steganografi dan Fungsi XOR”. 2006.

[2] Xu, Jun. “Secret Sharing Schemes with General Access Structure Based on MSPs,”, 2007.

[3] http://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf

[4] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm

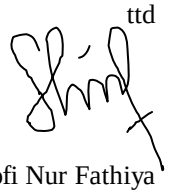
[5] http://www.ccse.kfupm.edu.sa/~akalvi/myweb/9.pdf

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, 8 Mei 2011

ttd



Shofi Nur Fathiya
13508084