Aplikasi Kriptografi Visual Untuk Sistem Veto

Fadhil Muhtadin - 13510070
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510070@std.stei.itb.ac.id

***Abstrak*—Kriptografi visual adalah metode untuk mengenkripsi sebuah citra dengan membaginya ke dalam sejumlah bagian yang hanya dapat didekripsi ketika bagian-bagian tersebut digabungkan. Dengan metode ini, banyak aplikasi yang dapat digunakan. Makalah ini akan membahas salah satu kemungkinan aplikasinya yakni untuk sistem veto. Untuk itu diperlukan skema pembagian rahasia dengan ambang batas tertentu dimana sejumlah partisipan dapat menyatakan ya maupun tidak untuk merepresentasikan pilihan menggunakan hak veto. Makalah ini juga membahas kemungkinan serangan dan optimasi untuk skema tersebut.**

***Kata Kunci*—Kriptografi visual, veto, skema pembagian rahasia, pixel.**

I. PENDAHULUAN

Kriptografi yang berasal dari kata dalam bahasa yunani "*kriptos*" yang berarti tersembunyi dan "*graphein*" yang berarti tulisan adalah sebuah ilmu yang mempelajari teknik komunikasi antara 2 pihak dimana komunikasi tersebut aman dan tersembunyi dari pihak ketiga. Kriptografi sebelum era digital hampir sama dengan enkripsi, yakni teknik mengubah informasi yang dapat dibaca menjadi tidak dapat dibaca. Namun, semenjak komputer mulai berkembang pesat, ilmu kriptografi menjadi semakin kompleks dan aplikasinya semakin luas. Bahkan tidak hanya digunakan dalam komunikasi saja. Misalnya, kriptografi dapat digunakan untuk membubuhkan tanda tangan digital untuk membuktikan keabsahan suatu dokumen atau watermark untuk keaslian hak cipta suatu karya.

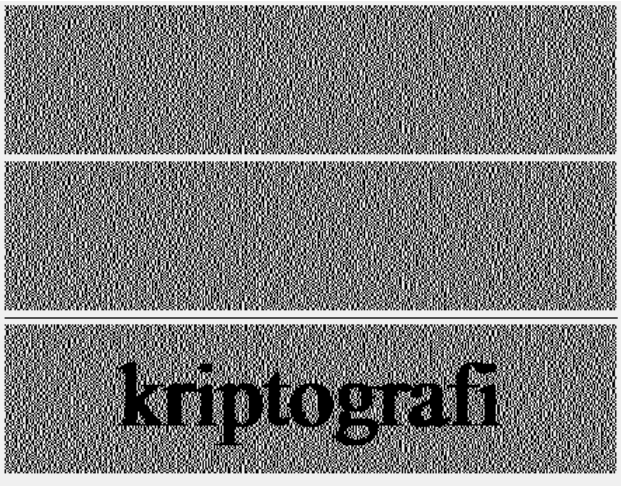
Salah satu kemungkinan aplikasi kriptografi yang tidak konvensional adalah penggunaannya dalam sistem veto. Veto adalah sebuah hak atau kekuatan untuk menolak keputusan oleh suatu badan hukum. Biasanya veto digunakan dalam proses legislatif suatu negara, seperti halnya pada Amerika Serikat. Pada sistem veto, suatu anggota badan lembaga memiliki hak untuk menolak secara sepihak keputusan yang akan diambil oleh lembaga tersebut. Keputusan baru dapat diambil jika semua atau sejumlah anggota yang memenuhi batas minimal telah menyetujuinya. Untuk dapat mengaplikasikan sistem ini, diperlukan kriptografi visual dengan skema pembagian rahasia.

Dalam kriptografi kita mengenal sebuah skema yang disebut skema pembagian rahasia (secret sharing atau secret splitting). Skema ini merupakan sebuah metode yang memungkinkan pendistribusian sebuah rahasia kepada beberapa partisipan yang masing-masing memegang bagian dari rahasia atau yang biasa disebut *share*. Skema ini menjawab sebuah permasalahan dalam dunia kriptografi yang dikenal sebagai masalah 6 perampok, dimana terdapat 6 orang perampok yang menyimpan hasil harta mereka kedalam satu akun bank yang sama. Namun, karena perampok ini tidak saling percaya satu sama lain, mereka meminta pihak bank untuk membagi kode PIN akun mereka supaya uang hanya bisa di ambil jika ada minimal 2 atau lebih perampok yang merangkainya menjadi kode PIN yang utuh.

Skema pembagian rahasia ini pada umumnya melibatkan sejumlah n partisipan yang memegang bagian atau disebut juga dengan *share* dan seorang *dealer* yang melakukan pembagian rahasia. *Dealer* ini harus merupakan pihak yang dapat dipercaya. Dalam salah satu skema pembagian rahasia yang disebut skema ambang batas, tidak dibutuhkan semua bagian untuk merekonstruksi rahasia melainkan hanya sejumlah minimal t (*threshold*) dari n partisipan dimana t <= n.

Selanjutnya untuk aplikasi pada sistem veto, skema pembagian rahasia ini perlu dapat dilakukan pada metode kriptografi visual. Kriptografi visual itu sendiri adalah sebuah teknik kriptografi dimana informasi visual seperti gambar, teks, dll dapat dienkripsi sedemikian rupa sehingga proses dekripsi tidak membutuhkan komputer, melainkan hanya proses mekanikal biasa. Proses dekripsi tidak bergantung pada persepsi visual komputer melainkan pada indra pengelihatan manusia.

Teknik ini pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka memperkenalkan skema secret sharing visual dimana sebuah gambar dapat dipecah menjadi sejumlah n *share* yang dicetak pada transparansi yang berbeda, sehingga gambar rahasia hanya dapat dilihat bila semua n *share* ditumpuk. Namun bila hanya n-1 atau kurang *share* yang ditumpuk, gambar tersebut tidak akan muncul.



Gambar 1 – 2 buah *share* yang ditumpuk menghasilkan gambar rahasia

II. DASAR TEORI

A. Model Kriptografi Visual

Sebuah gambar digital terbagi-bagi atas elemen terkecil yakni pixel. Pada model kriptografi visual yang paling sederhana, tiap pixel ini dapat berupa angka biner 0 atau 1 yang merepresentasikan putih atau hitam. Gambar ini dapat dikenali manusia dari pixel hitam yang menjadi sebuah bentuk atau tulisan dengan latar belakang putih. Sebuah gambar berukuran mxn pixel kemudian dapat direpresentasikan sebagai matriks mxn yang tiap elemennya merupakan bit pixel. Gambar tersebut lalu dipecah menjadi 2 atau lebih gambar dimana tiap *share* merupakan subset dari gambar asli.

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

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

Gambar 2 – Contoh representasi matriks gambar yang dipecah ke dalam 2 bagian

Namun, metode ini dianggap kurang aman. Adi Shamir dan Moni Naor pada makalahnya meperkenalkan model yang lebih baik. Pada model mereka, tiap pixel dibagi lagi ke dalam blok-blok subpixel yang lebih kecil. Sehingga tiap pixel tidak direpresentasikan sebagai sebuah elemen matriks melainkan sebagai m buah elemen matriks.

Subpixel-subpixel ini kemudian dibagi ke dalam n buah bagian yang tiap bagian terdiri atas m buah subpixel hitam dan putih. Hasilnya adalah sebuah matriks boolean nxm S = $[s_{ij}]$ dimana s_{ij} = 1 jika dan hanya jika subpixel ke-j pada transparansi ke-i adalah hitam. Ketika transparansi $i_1,i_2,\ldots,i_r$ ditumpuk, kita akan mendapat *share* gabungan yahg subpixel hitamnya direpresentasikan oleh boolean "or" dari baris $i_1,i_2,\ldots,i_r$ pada S.

Kemudian, level keabuan pada pixel kombinasi ini ditentukan oleh Hammimg Weight H(V) dari m-vektor V yang telah di-"or" tersebut. Definisi formal dari Hamming weight itu sendiri adalah: jumlah simbol non-zero pada suatu sekuens simbol. Sehingga untuk representasi biner, hamming weight adalah banyaknya bit "1" pada sekuens biner. Sedangkan definisi dari m-vektor yang telah di-"or"-kan adalah m-vektor dari sebuah matriks berukuran nxm dimana tiap tupel terdiri atas hasil operasi boolean OR pada vektor kolom nx1 yang bersangkutan. Level keabuan ini diinterpretasikan sebagai hitam oleh manusia jika H(V) >= d dan putih jika H(V) < d – αm untuk batas tetap 1 <= d <= m dan selisih relatif α > 0.

Definisi formal yang diberikan oleh Shamir dan Naor untuk skema kriptografi visual adalah sebagai berikut:

Solusi atas skema k dari n pembagian rahasia terdiri atas 2 koleksi matriks boolean nxm C0 dan C1. Untuk membagi pixel putih, *dealer* memilih satu matriks secara acak dari C0, dan untuk pixel hitam, dari C1. Matriks yang terpilih mendefinisikan warna dari m subpixel dari tiap n transparansi. Solusi dianggap valid bila kondisi berikut terpenuhi :

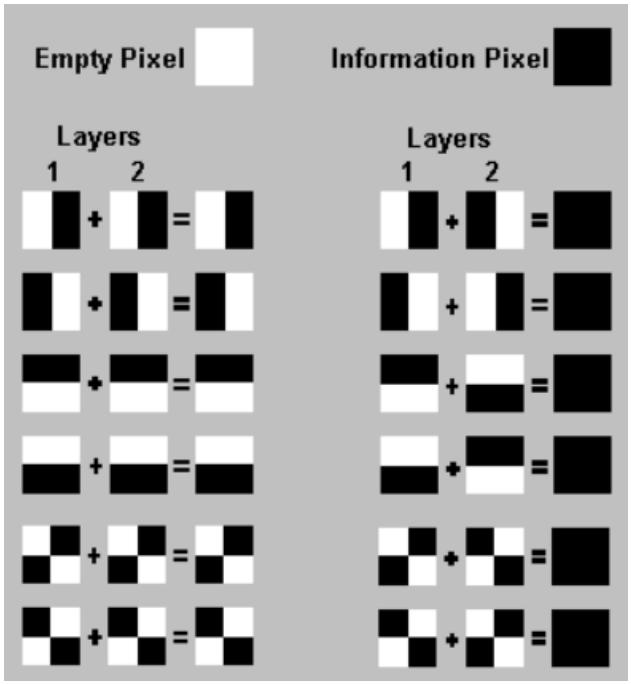
1. Untuk tiap S dalam C0, "or" V dari tiap k dari n baris memenuhi H(V) <= d – αm.
2. Untuk tiap S dalam C1, "or" V dari tiap k dari n baris memenuhi H(V) >= d.
3. Untuk tiap subset $\{i_1,i_2,\ldots,i_q\}$ dari {1,2,…,n} dengan q < k, 2 koleksi matriks Dt berukuran qxm untuk t ϵ {0,1} yang diambil dari membatasi tiap matriks nxm dalam Ct (dimana t = 0,1) ke dalam baris $i_1,i_2,\ldots,i_q$ adalah tidak dapat dibedakan dalam artian mereka mengandung matriks yang sama dengan frekuensi yang sama.

Kondisi ketiga ini yang mengimplikasikan bahwa jika kita hanya memiliki kurang dari k buah bagian, kita tidak bisa mendapatkan informasi rahasia dari hasil rekonstruksinya.

Dalam model ini, beberapa parameter yang penting adalah :

1. m, yakni jumlah pixel dalam sebuah bagian. Ini merepresentasikan resolusi yang hilang dari gambar asli ke gambar yang terbagi.
2. α, yakni selisih relatif Hamming weight antara *share* kombinasi dari pixel putih dan hitam. Ini merepresentasikan kontras gambar.
3. r, yakni ukuran koleksi matriks C0 dan C1, parameter ini tidak memiliki pengaruh terhadap kualitas gambar.

Sebagai contoh, sebuah model dimana tiap pixel dibagi ke dalam 4 subpixel dan gambar asli dibagi menjadi 2 bagian dapat memiliki beberapa state seperti gambar berikut ini



Gambar 3 – Overlay beberapa state 2 buah *share*

Pada contoh diatas, seorang pengguna akan menginterpretasikan warna hitam bila subpixel pada *share* 1 merupakan invers dari subpixel dari *share* 2 sehingga ketika ditumpuk, gabungannya akan menghasilkan pixel yang seluruhnya hitam.

B. Skema Kriptografi Visual Ambang Batas Dengan Veto

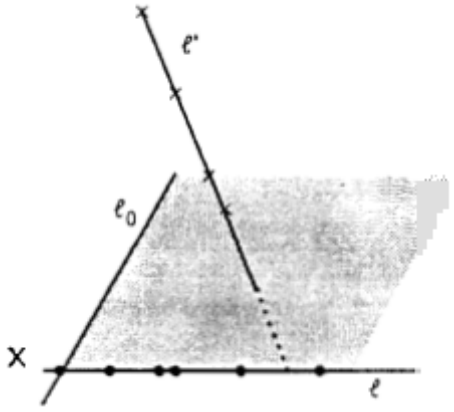
Dalam sebuah skema ambang batas (k,h,n) dengan veto, terdapat seorang *dealer* D, mesin rekonstruksi R, dan sejumlah n partisipan p_1, p_2, …, p_n. Pada fase distribusi rahasia, D akan menghasilkan *share* $v_i = (v_i^p, v_i^n)$ secara acak dari suatu gambar rahasia untuk i = 1,2,…,n dimana v^p adalah *share* positif, dan v^n adalah *share* negatif. Selanjutnya pada fase rekonstruksi, tiap partisipan diwajibkan untuk mengirimkan v^p atau v^n kepada R. Kita asumsikan bahwa R dapat dipercaya, jika R menerima sejumlah k-1 atau kurang bagian, R tidak bisa mendapatkan informasi apapun terhadap gambar rahasia. Jika R menerima sejumlah h atau lebih *share* negatif, R tidak dapat merekonstruksi gambar rahasia. Selain itu, jika R menerima sejumlah k atau lebih *share* positif dan h-1 atau kurang *share* negatif, R dapat merekonstruksi gambar rahasia.

Dengan demikian, kita dapat membuat sistem veto dimana tiap partisipan akan mendapat 2 macam bagian dari gambar rahasia, yang satu menyatakan "ya" dan yang satu menyatakan "tidak". Tiap partisipan kemudian menyerahkan salah satu *share* yang mereka miliki sesuai pilihan mereka kepada mesin rekonstruksi. Jika jumlah yang menyatakan "tidak" mencapai ambang batas, maka gambar rahasia tidak dapat direkonstruksi dan pengambilan keputusan gagal.

C. Skema Beutelspacher

Beutelspacher dalam makalahnya memperkenalkan sebuah skema ambang batas (k,h,n) menggunakan geometri proyektif. Berikut adalah skemanya :

Pada sebuah geometri 3 dimensi yang kita batasi pada ruang proyeksi 3-dimensi P = PG(3,q) pada orde q, ambil titik X yang merupakan rahasia. Pilih sebuah garis l_0 melalui X. Definisikan P sebagai himpunan titik pada garis l yang memotong l_0 pada X, dan N sebagai himpunan titik dari l' ∩ $<l,l_0>$ pada garis l' yang miring terhadap l. Kita gunakan notasi <U> sebagai span dari U pada ruang proyeksi.



Gambar 4 – Proyeksi Beutelspacher

Kemudian, kita definisikan protokol berikut : jika himpunan U dari positif dan negatif adalah aktif, maka sistem akan mengkalkulasi <U> dan mengambil perpotongannya dengan l_0. Jika <U> ∩ l_0 adalah sebuah titik, maka sistem akan mengambilnya sebagai sebuah rahasia. Contohnya pada ambang batas (2,2), akan ada 4 kasus :

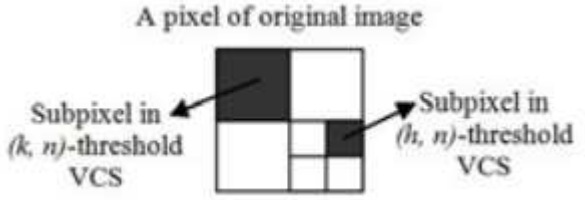
1. Jika minimal 2 titik positif aktif, tapi tidak ada titik negatif yang aktif, maka sistem akan mengambil l ∩ l_0 = X sebagai rahasia.
2. Jika minimal 2 titik positif aktif dan 1 titik Y dari negatif aktif, maka sistem akan mendapat bidang E = <l,Y>; karena Y ∉ $<l,l_0>$ maka E ≠ $<l,l_0>$ sehingga E hanya memotong l_0 pada X.
3. Jika minimal 2 titik positif dan 2 titik negatif aktif, maka sistem mengkomputasi <l,l'> = P, memotongnya dengan l_0 dan mendapat l_0, sehingga rahasia tidak dapat diambil.
4. Jika maksimal 1 titik positif dan minimal 2 titik negatif aktif, maka sistem akan mendapat titik yang berbeda dari X.

D. Distribusi Rahasia Skema Ambang Batas Veto

Massoud Hadian Dehkordi dan Abbas Cheraghi dalam makalahnya mengusulkan metode pembagian rahasia menggunakan skema beutelspacher yang telah dijelaskan. Metode mereka adalah sebagai berikut:

Untuk menghasilkan *share* positif $v_1^p, v_2^p, \ldots, v_n^p$, *dealer* D mengaplikasikan skema kriptografi visual ambang batas (k,n) dengan jumlah pixel m dan matriks basis C0 dan C1 untuk pixel putih dan hitam.

Untuk menghasilkan *share* negatif $v_1^n, v_2^n, \ldots, v_n^n$, *dealer* D mengaplikasikan skema kriptografi visual ambang batas (h,n) dengan jumlah pixel m' dan matriks basis C0' dan C1' untuk pixel putih dan hitam. Namun, D hanya mengaplikasikannya pada subpixel bukan pixelm dari gambar asli, seperti pada gambar dibawah



Gambar 5 – Skema pengambilan pixel dan subpixel untuk distribusi rahasia

Disini, $m = 2^{C(n,k-1)-1}$ sedangkan $m' = 2^{C(n,h-1)-1}$. Dengan menggunakan C' hanya pada subpixel gambar asli, ketika terdapat h atau lebih *share* negatif, gambar yang dihasilkan menjadi hitam semua sehingga tidak dapat direkonstruksi.

Dengan demikian, skema kriptografi visual ambang batas untuk veto yang telah dijabarkan sebelumya, ditambahkan dengan metode distribusi rahasia ini dapat disimpulkan dengan protokol berikut:

Protokol : Jika diberikan sejumlah *share* positif dan negatif, mesin rekonstruksi R akan menyusunnya sehingga R mendapatkan gambar rahasia darinya atau gambar hitam.

Fase rekonstruksi :

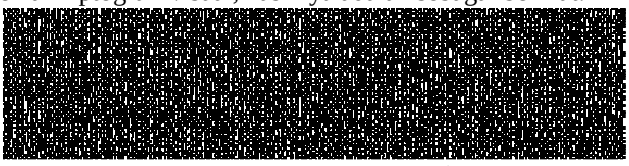
Pada fase rekonstruksi, subset partisipan mengirimkan vp atau vn transparansi kepada R.

1. Jika R menerima sejumlah k-1 atau kurang bagian, maka R tidak memiliki informasi atas rahasia.
2. Jika R menerima h atau lebih *share* negatif, maka R mendapatkan gambar hitam dan gambar asli tidak dapat direkonstruksi.
3. Jika R mendapat k atau lebih *share* positif dan h-1 atau kurang *share* negatif, maka R dapat merekonstruksi gambar rahasia dengan kontras minimal 1/(m.m').

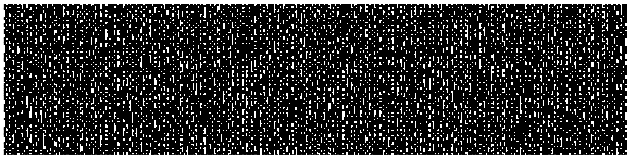
III. APLIKASI

A. Pengujian

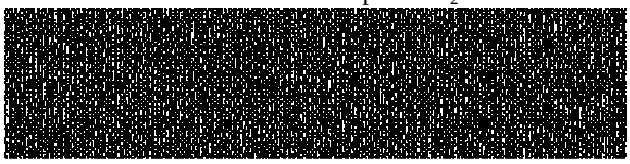
Dengan menggunakan library kriptografi visual yang dapat diunduh di internet, dilakukan uji coba terhadap skema kriptografi visual, hasilnya adalah sebagai berikut.



Gambar 6 – *share* positif v_1^p



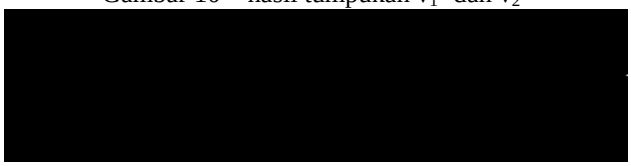
Gambar 7 – *share* positif v_2^p



Gambar 8 – *share* negatif v_1^n

Gambar 9 – *share* negatif v_2^n

Gambar 10 – hasil tumpukan v_1^p dan v_2^p



Gambar 11 – hasil tumpukan v_1^n dan v_2^n

Dari hasil tersebut, terbukti bahwa jika terdapat sejumlah minimal partisipan yang memilih "tidak" maka gambar yang dihasilkan adalah hitam penuh, sehingga gambar asli tidak dapat direkonstruksi. Hal tersebut cukup menyakinkan bahwa skema ini dapat digunakan untuk sistem veto.

B. Kemungkinan Serangan

Pada skema beutelspacher, dinyatakan bahwa ada kemungkinan serangan. Pada contohnya yakni skema (2,2,n), misalkan mesin rekonstruksi R tidak dapat dipercaya, R mendapatkan (v_1^p, v_2^p, v_1^n, v_2^n) yakni 2 buah *share* positif dan 2 buah *share* negatif, maka R dapat mencoba semua kemungkinan subset dari himpunan ini, maka R bisa mendapatkan gambar rahasia dari 2 buah *share* positif tersebut yakni (v_1^p, v_2^p).

Dengan demikian, skema yang ditawarkan untuk sistem veto ini juga memiliki kelemahan yang sama. Yakni jika seseorang mengetahui himpunan $P \cup N$ atau *share* positif dan negatif yang aktif, maka orang tersebut dapat melakukan brute force attack terhadap semua kemungkinan subset himpunan tersebut apabila $|P| >= k$ hingga ditemukan gambar rahasia.

Sampai saat ini, satu-satunya cara untuk mengantisipasi serangan ini adalah dengan menghindari kemungkinan *share-share* tersebut baik positif maupun negatif dari kebocoran informasi, sehingga tidak ada orang yang tidak berkepentingan bisa mendapatkan satupun *share* tersebut. Ini dapat dicapai bila *dealer* dan mesin rekonstruksi

adalah pihak yang dapat dipercaya, yang mana hal tersebut sudah menjadi asumsi awal untuk pembentukan skema kriptografi visual ambang batas untuk sistem veto ini.

C. Kemungkinan Optimasi

Optimasi pada skema kriptografi visual ditentukan kebanyakan dari parameter ekspansi pixel m dan kontras relatif α. Ekspansi pixel m merepresentasikan resolusi yang hilang pada gambar bagian dari gambar asli, maka kita ingin agar m sekecil mungkin. Sedangkan nilai α perlu sebesar mungkin untuk memudahkan pengelihatan.

Masalah hilangnya nilai kontras terjadi akibat efek "*extra greying*" yang terjadi pada gambar bagian. Ini karena gambar bagian bukan merupakan reproduksi dari gambar asli melainkan ekspansi dari gambar asli. Pixel hitam akan tetap hitam pada kondisi tertentu sedangkan pixel putih dapat menjadi abu-abu karena subpixel hitam yang timbul pada gambar bagian. Secara umum, skema ambang batas (2,2) akan menghasilkan kontras terbaik. Untuk mengatasi hal ini, dapat menggunakan metode "Cover" semi-group operation yang merupakan perbaikan dari metode awal yang diusulkan Shamir dan Naor.

IV. KESIMPULAN

Kriptografi memiliki banyak sekali aplikasi, tidak hanya dalam bidang komunikasi rahasia. Salah satunya adalah pengembangan skema kriptografi visual untuk diterapkan pada sistem veto.

Pada skema ini, sejumlah partisipan diberikan dua macam *share* oleh *dealer*, yakni yang satu untuk menyatakan "ya" dan yang satu untuk menyatakan "tidak". Pada fase rekonstruksi, sejumlah partisipan akan menyerahkan *share* yang mereka pilih kepada mesin rekonstruksi, mesin ini lalu akan mencoba merekonstruksi gambar rahasia. Jika ada sejumlah minimal partisipan yang menggunakan hak vetonya dan menyatakan "tidak", maka hasilnya adalah gambar hitam yang tidak bermakna apapun. Namun jika jumlah yang menggunakan hak vetonya tidak mencapai batas minimal, gambar rahasia dapat direkonstruksi dan keputusan dapat diambil.

Namun, skema ini bukanlah sempurna, masih ada kelemahan. Yakni *share* yang diproduksi tidak boleh sama sekali diketahui oleh pihak yang tidak berwenang. Jika ada orang pihak luar yang mengetahuinya, dapat dilakukan serangan brute force terhadapat himpunan *share* yang diketahui tersebut untuk mendapatkan gambar rahasia. Untuk itu, diperlukan seorang *dealer* dan pihak yang merekonstruksi ukang gambar yang dapat dipercaya untuk tidak membocorkan informasi.

Akhir kata, skema kriptografi visual untuk sistem veto ini masih perlu banyak perbaikan, namun dari hasil pengujian awal sudah menghasilkan harapan bahwa sistem ini punya harapan dan dapat dikembangkan menjadi sistem yang lebih canggih lagi sehingga mungkin dapat menjawab persoalan yang dihadapinya saat ini.

DAFTAR REFERENSI

[1] Moni Naor & Adi Shamir, "Visual Cryptography", Eurocrypt94.

[2] Albrecht Beutelspacher, "How To Say No", Justus-Liebig-Universitat GieBen : Jerman, 1990.

[3] Jim Cai, "*A Short Survey On Visual Cryptography Schemes*".

[4] Andreas Klein, "How to say yes, no and maybe with visual cryptography", Ghent University : Belgium, 2008.

[5] Massoud Hadian Dehkordi & Abbas Cheraghi, "Visual Cryptography Schemes with Veto Capabilities", *Iran*, 2008.

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, 20 Mei 2013

ttd

Fadhil Muhtadin
13510070