Kriptografi Visual Menggunakan Algoritma Berbasiskan XOR dengan Menyisipkan pada K-bit LSB Gambar Sampul

Yusuf Rahmatullah
Program Studi Teknik Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13512040@std.stei.itb.ac.id

***Abstract*—Kriptografi visual terhadap sebuah pesan berbentuk gambar yang kemudian disisipkan ke dalam gambar lainnya (steganografi). Penciptaan gambar acak yang akan dikirm menggunakan skema berbasiskan XOR untuk menciptakan setiap elemen warna pada gambar. Gambar acak kemudian disisipkan ke dalam gambar lainnya untuk menghilangkan kecurigaan terhadap gambar acak. Penyisipan gambar acak ke dalam gambar sampul menggunakan 2-bit LSB pada gambar sampul sebagai pelindung pesan gambar untuk meningkatkan nilai PSNR.**

***Keywords*—Kriptografi Visual; Steganografi; Skema Berbasiskan XOR**

I. PENDAHULUAN

Penggunaan kriptografi di masa ini sudah sangat banyak. Penggunaan kriptografi adalah untuk meningkatkan keamanan penyampaian pesan dari satu instansi ke instansi lain. Kriptografi mengikuti perkembangan zaman. Kriptografi modern adalah kriptografi digital yaitu menggunakan bit atau byta dalam enkripsi dan dekripsinya.

Salah satu bidang kriptografi modern adalah kriptografi visual. Pada kriptografi visual, pesan gambar atau pesan rahasia yang akan dikirimkan dari suatu tempat ke tempat lain diubah atau dienkripsi ke dalam bentuk gambar acak. Gambar acak ini kemudian dikirimkan kepada pihak penerima dengan menggunakan kiriman paket atau menggunkan faksimil. Dekripsi gambar acak dengan menyatukan gambar acak. gambar acak harus dicetak pada kertas transparan agar gambar dapat didekripsi.

Kriptografi visual diadopsi secara digital dengan menggunakan komputer. Gambar dengan warna hitam putih direpresentasikan dengan bit 0 dan 1. Kriptografi visual dengan menggunakan komputer memudahkan pengiriman gambar acak dan deksripsi gambar acak dilakukan secara digital. Penggunaan komputer memperkecil kemungkinan gambar hilang atau rusak.

Komputer masa kini dapat menyimpan gambar dengan kedalaman warna sebesar 16 juta warna. Kriptografi visual menyesuaikan dengan kebutuhan pengguna. Kriptografi visual tidak lagi dilakukan terhadap gambar hitam dan putih namun dilakukan terhadap gambar dengan kedalaman 16 juta warna. keadaan ini menghasilkan gambar acak dengan kedalaman 16 juta warna.

Gambar acak menimbulkan rasa curiga bagi pihak ketiga yang melihat gambar tersbeut. Gambar acak tidak memiliki makna sehingga mudah saja bagi orang untuk mencurigai gambar tersebut. Jika pihak ketiga memiliki kedua gambar acak yang diciptakan pada proses enkripsi, maka dengan mudah pihak ketiga tersebut mendapatkan gambar rahasia dengan menggabungkan kedua gambar tersebut.

Kriptografi visual dengan skema OR kotak 2x2 memiliki kelemahan pada gambar hasil dekripsi. Gambar hasil dekripsi berbeda dengan gambar rahasia asli. Gambar hasil dekripsi memiliki *noise. Noise* pada gambar dihasilkan dari penyatuan dua kotak 2x2 pada kedua gambar sampul. Gambar dengan warna hitam putih akan tetap terlihat walaupun terdapat *noise*.

Kriptografi visual dengan skema XOR menutupi kelemahan pada skema tersebut. Kriptografi visual skema XOR memberikan kepastian warna yang sama untuk setiap elemen warna pada gambar rahasia dan gambar hasil dekripsi. Hal ini dikarenakan algoritma yang digunakan adalah XOR untuk setiap elemen gambar. Setiap elemen warna pada gambar acak pertama di XOR-kan dengan setiap elemen pada gambar acak kedua sehingga menghasilkan gambar hasil dekripsi yang sama persis dengan gambar rahasia.

Steganografi merupakan salah satu bidang kriptografi yaitu menyisipkan pesan pada sebuah gambar. Gambar yang telah disisipi pesan tidak terlihat perbedaannya sehingga pihak ketiga tidak akan curiga bahwa gambar tersebut telah disisipi suatu pesan. Pesan yang telah disisipi dapat diekstraksi dari gambar tersebut oleh pihak penerima. Penyisipan ini dapat dilakukan terhadap pesan yang terenkripsi.

Pada kriptografi modern, pesan dari steganografi diubah ke dalam bentuk bit dan disisipkan ke dalam bit di setiap elemen gambar. Pesan dalam bentuk bit tersebut disisipkan ke dalam LSB (*Least Significant Bit*) pada setiap elemen gambar pada gambar sampul. Pesan yang disisipkan pada gambar sampul merupakan kumpulan bit, sehingga data apapun pada komputer

dapat disisipkan ke dalam gambar sampul dengan syarat ukuran pesan lebih kecil dari ukuran gambar sampul.

Gambar acak hasil enkripsi pada kriptografi visual merupakan kumpulan bit yang dapat disisipkan ke dalam sebuah gambar sampul seperti penyisipan sebuah pesan ke dalam gambar sampul pada steganografi. Hal ini dilakukan untuk mengurangi kecurigaan pihak ketiga terhadap gambar acak hasil enkripsi gambar rahasia.

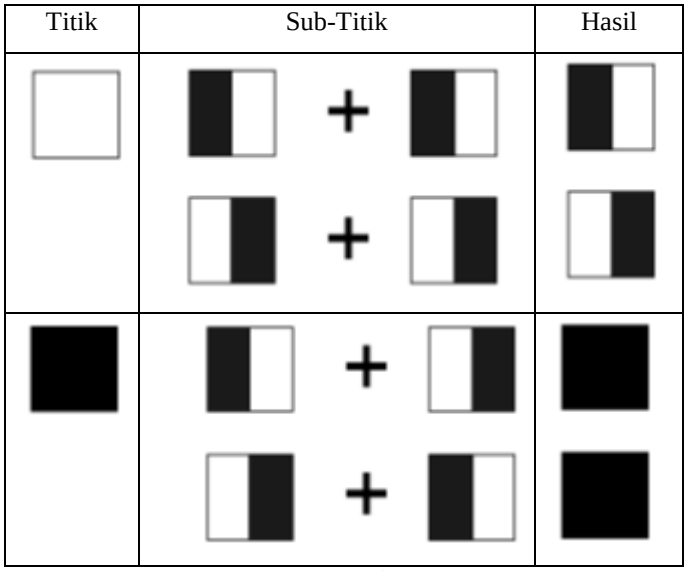
II. DASAR TEORI

A. Kriptografi Visual Tradisional

Kriptografi visual adalah salah satu bidang kriptografi dalam bidang visual. Kriptografi visual mengenkripsi suatu pesan informasi berupa teks atau gambar ke dalam sejumlah gambar acak yang dikirimkan ke pihak penerima. Gambar acak tersebut didekripsi secara mekanik yaitu dengan menempelkan seluruh gambar acak. Gambar acak harus dicetak pada kertas transparan.

Kriptografi visual pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka memperkenalkan cara baru dalam mengirimkan pesan rahasia. Mereka membagi pesan rahasia pada gambar ke dalam beberapa gambar acak yang masing-masing dicetak pada kertas transparan. Kertas transparan tersebut lalu disatukan sehingga setiap titik pada gambar acak saling menimpa dan memunculkan gambar baru, yaitu gambar hasil dekripsi.

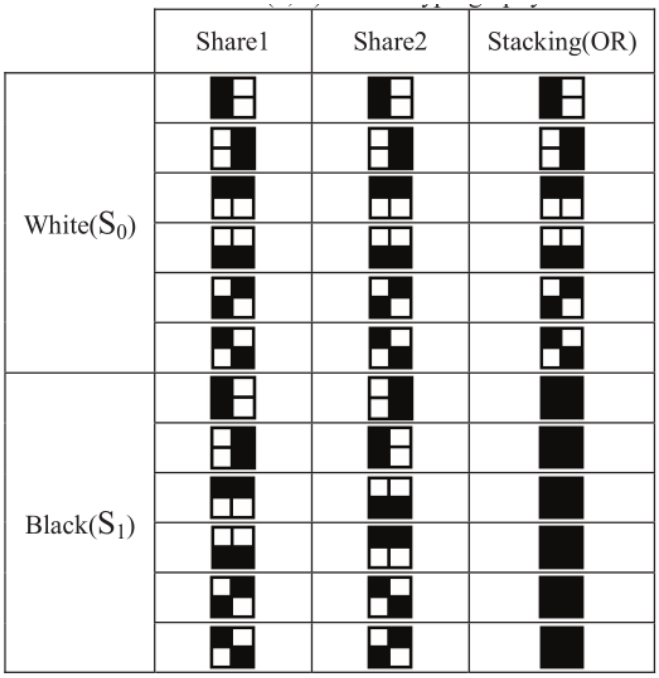
Kriptografi visual tradisional menggunakan gambar dengan warna hitam dan putih. Setiap titik elemen gambar pesan dibuat ke dalam sub-titik pada gambar acak. Sub-titik ini merepresentasikan satu titik pada gambar asli. Salah satu contoh model pembentukan sub-titik menjadi titik adalah sebagai berikut :



Sumber : Munir, R. Pengenalan Kriptografi Visual

Model di atas adalah salah satu contoh pembentukan titik pada gambar acak dengan menggunakan 2 sub-titik. Titik putih direpresentasikan ke dalam titik dengan warna hitam dan putih sedangkan titik hitam di representasikan dengan warna hitam utuh. Representasi ini menyebabkan warna putih pada hasil dekripsi gambar mengandung warna hitam. Warna hitam pada titik putih ini disebut *noise*.

Model kriptografi visual berkembang menjadi n^2 sub-titik. sub-titik berbentuk persegi dengan ukuran n untuk menjaga keaslian ukuran gambar asli. Gambar acak akan memiliki ukuran n^2 kali lebih besar dari gambar asli. Di bawah ini adalah contoh model kriptografi visual dengan ukuran 4 sub-titik.



Sumber : Mostaghim, M., Boostani, R., CVC : Chaotic Visual Cryptography to Enhance Steganography

Model di atas menunjukkan 6 buah variasi 4 sub-titik pada gambar acak yang dapat diciptakan dari 1 titik pada gambar asli. Banyaknya variasi dapat ditambahkan sesuai dengan kebutuhan. Model kriptografi visual dengan 9 sub-titik dapat memiliki lebih dari 60 variasi.

Kriptografi visual memiliki dua buah skema dekripsi yang berbeda, yaitu skema (N, N) dan skema (k, N). Kriptografi visual dengan skema (N, N) adalah kriptografi visual yang menenkripsi gambar asli menjadi N buah gambar acak dan dekripsi membutuhkan seluruh gambar acak. Sedangkan kriptografi visual dengan skema (k, N) adalah krpitografi visual yang mengenkripsi gambar asli menjadi N buah gambar acak namun hanya dibutuhkan k gambar acak untuk mendeskripsi gambar acak untuk mendapatkan hasil.

Kriptografi visual dengan skema (N, N) memiliki keuntungan dalam hal keamanan. Pihak ketiga yang ingin memecahkan gambar rahasia harus memliki seluruh gambar. Skema (N, N) juga memiliki kelemahan. Pengirim pesan harus memastikan bahwa seluruh gambar acak berhasil diterima oleh penerima. Pihak ketiga bisa saja mencuri salah satu gambar

acak sehingga penerima tidak dapat mendapatkan informasi seutuhnya.

Skema (k, N) memiliki keuntungan dalam distribusi gambar acak. Gambar acak dapat dikirmkan pengirim dengan secara paket-paket kecil berukuran k-1 gambar acak. Hal ini menyebabkan pihak ketiga yang mencoba mengambil salah satu paket tidak dapat mengetahui informasi pada gambar acak. Kelemahan dari skema (k, N) adalah keamanan. Pihak ketiga hanya membutuhkan k buah gambar acak untuk mendekripsi gambar acak dan mendapatkan informasi.

B. Kriptografi Visual Modern

Kriptografi visual modern adalah kriptografi visual yang dilakukan pada gambar digital. Gambar digital direpresentasikan dengan menggunakan bit pada komputer. Gambar dengan warna hitam putih direpresentasikan dalam bit 1 dan 0. Gambar hitam putih pada kriptografi visual modern disebut juga gambar biner.

Pembentukan gambar acak pada kriptografi visual modern menggunakan operasi OR dan XOR untuk setiap titik atau elemen gambar. Model kriptografi visual modern disesuaikan dengan model kriptografi visual tradisional. Kriptografi visual modern yang paling sederhana adalah dengan model 1 titik ke 1 titik.

Proses dekripsi gambar acak dilakukan dengan menggunakan perhitungan digital. Setiap titik pada gambar acak dilakukan operasi OR dan XOR untuk mendapatkan titik pada gambar asli. Kriptografi visual modern hanya menyediakan skema (N, N) dengan N=2. Skema (k, N) dapat dilakukan dengan syarat k=2 dan setiap titik hitam pada gambar asli direpresentasikan sama pada setiap titik di gambar acak. Hal ini dilakukan agar tidak ada informasi yang hilang pada proses dekripsi dengan menggunakan 2 buah sembarang gambar acak.

gambar pada komputer terdiri dari titik-titik yang disebut elemen gambar atau *picture element (pixel)*. Setiap elemen gambar terdiri dari n-bit yang merepresentasikan warna. Gambar hitam putih atau gambar biner memiliki 1-bit warna pada setiap elemen gambarnya. Gambar berwarna memiliki 3 buah warna dasar di setiap elemen gambarnya. Warna dasar ini adalah merah, hijau, dan biru. Setiap warna dasar direpresentasikan dalam ukuran 1 byte (8-bit). Oleh karena itu, setiap elemen gambar berukuran 3 byte yang terdiri dari 1 byte warna merah, 1 byte warna hijau, dan 1 byte warna biru. Kombinasi dari seluruh warna dasar adalah sebanyak 2^{24} atau sebanyak 16 juta warna. Jumlah bit pada setiap elemen gambar disebut juga dengan kedalaman warna.

C. Steganografi

Steganografi adalah salah satu cabang kriptografi yaitu menyisipkan pesan dalam sebuah gambar. Steganografi dalam kriptografi modern menggunakan bit dalam merepresentasikan pesan rahasia dan gambar sampul yang digunakan. Steganografi modern menyisipkan setiap bit pesan pada LSB (*Least Significant Bit)* pada elemen gambar. Satu karakter pesan mengandung 8 bit yang akan disisipkan ke dalam 8 elemen gambar dengan kedalaman 8-bit atau dapat ke dalam 3 elemen gambar dengan kedalaman 24-bit.

Steganografi dapat menyimpan pesan sebanyak k-bit pada LSB setiap byte di elemen gambar. Steganografi yang sederhana menggunakan 1-bit pesan untuk disisipkan ke dalam setiap LSB elemen gambar. Perubahan 1 bit pada LSB elemen gambar tidak mempengaruhi kualitas gambar. Namun, ukuran gambar sampul minimal harus 8 kali lebih besar dari ukuran pesan. Steganografi dengan k>1 mengurangi kualitas gambar karena jumlah bit yang berubah pada gambar sampul lebih banyak.

Kualitas gambar hasil steganografi dihitung dengan menggunakan PSNR (*Peak Signal-to-Noise Ratio)*. PSNR adalah perbandingan besarnya nilai maksimum sebuah *signal* dan *noise* akibat dari suatu operasi tertentu. PSNR biasanya digunakan untuk menghitung kualitas sebuah gambar yang dikompresi agar ukurannya menjadi kecil. PSNR dihitung dalam satuan dB. Semakin besar nilai PSNR semakin baik kualitas sebuah gambar. PSNR dihitung dengan rumus :

$$PSNR = 10 \bullet \log_{10}\left(\frac{MAX^2}{MSE}\right)$$

dimana MAX adalah nilai maksimum *signal* yaitu sebesar 2^n untuk gambar dengan kedalaman *n*-bit dan MSE (*Mean Squarred Error*) yaitu :

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

dimana *I* adalah gambar asli dan *K* adalah gambar yang memiliki *noise*.

III. METODE YANG DIAJUKAN

Kriptografi visual modern yang diajukan menggunakan skema (2, 2) dengan representasi titik 1-bit ke 1-bit menggunakan algoritma berbasiskan XOR. Gambar acak hasil enkripsi kemudian disisipkan ke dalam gambar sampul berbeda. Hal ini dimaksudkan untuk menghilangkan rasa curiga dari pihak ketiga yang melihat gambar acak secara langsung. Gambar acak yang tidak memiliki makna akan menimbulkan curiga bahwa pada gambar tersebut terdapat pesan rahasia. Sedangkan jika gambar tersebut disisipkan ke dalam sebuah gambar sampul, maka pihak ketiga tidak akan curiga ketika melihat gambar sampul yang telah disisipi pesan rahasia.

A. Proses Enkripsi Gambar Rahasia

Proses enkripsi gambar rahasia menjadi gambar acak dilakukan dengan langkah-langkah berikut :

Pertama :

Setiap nilai elemen gambar direpresentasikan menjadi $p_{i,j}$ dengan *i* dan *j* adalah posisi elemen gambar pada gambar rahasia dengan *i* adalah indeks pada panjang gambar dan *j* adalah indeks pada lebar gambar.

Kedua :

Ambil sembarang angka positif *r* yang tidak lebih dari nilai maksimal satu elemen gambar. Elemen gambar dengan kedalaman 24-bit memiliki nilai maksimal sebesar 16.777.215.

Ketiga :

Setiap nilai elemen gambar acak direpresentasikan menjadi $m_{i,j}$ dan $n_{i,j}$ dengan *m* adalah elemen gambar acak pertama dan *n* adalah elemen gambar acak kedua. Nilai $m_{i,j} = r$ dan nilai $n_{i,j} = m_{i,j}$ *XOR* $p_{i,j}$.

Keempat :

Ambil sembarang angka positif *r* lainnya. Ulangi langkah ketiga hingga seluruh nilai pada nilai pada *m* dan *n* terisi.

Kelima :

Sisipkan bit pada setiap elemen gambar *m* ke *k*-bit LSB elemen gambar sampul *c* dan setiap elemen gambar *n* ke *k*-bit LSB elemen gambar sampul *d*. Gambar sampul yang dapat digunakan harus memiliki ukuran minimal :

$$s_c = \frac{\gamma_m}{\gamma_c} \times \frac{8}{k} \times s_m$$

Keterangan :

s_c : ukuran gambar sampul (*panjang x lebar*)

s_m : ukuran gambar acak (*panjang x lebar*)

γ_c : kedalaman warna gambar sampul

γ_m : kedalaman warna gambar acak

k : banyaknya bit yang disisipkan ke dalam gambar sampul

B. Proses Dekripsi Gambar Acak

Proses dekripsi gambar acak menjadi gambar rahasia dilakukan dengan langkah-langkah berikut :

Pertama :

Ekstraksi *k*-bit pada setiap elemen gambar sampul *c* untuk mendapatkan gambar acak *m* dan ektraksi *k*-bit pada setiap elemen gambar smapul *d* untuk mendapatkan gambar acak *n*.

Kedua:

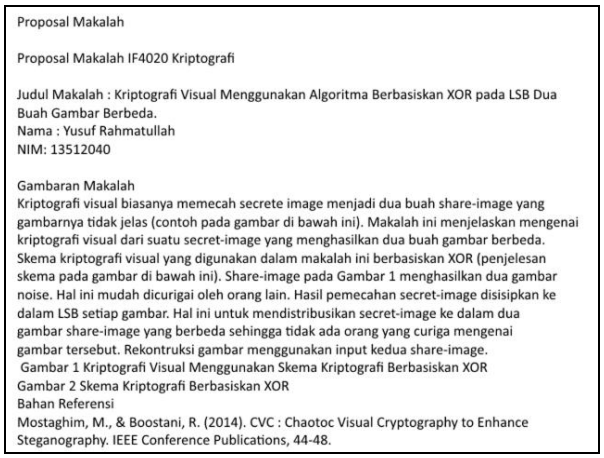
Elemen gambar rahasia $p_{i,j}$ didapatkan dari operasi XOR antara elemen gambar acak $m_{i,j}$ dengan elemen gambar acak $n_{i,j}$ sehingga didapatkan $p_{i,j} = m_{i,j}$ *XOR* $n_{i,j}$.

IV. Eksperimen dan Pembahasan Hasil

Percobaan dilakukan terhadap sebuah gambar rahasia dengan ukuran gambar rahasia 640x480 dengan kedalaman 24-bit. Penentuan *k*-bit ditentukan dengan menghitung ukuran gambar minimal yang dibutuhkan untuk menyimpan gambar pesan. Perhitungan *k*-bit dengan kedalaman warna gambar sampul 24-bit adalah sebagai berikut :

k-bit	Ukuran minimal gambar sampul	Ukuran minimal gambar sampul dengan rasio 4:3
1	2.457.600	1811x1358
2	1.228.800	1280x960
3	819.200	1046x784
4	614.400	906x679
5	491.520	810x608
6	409.600	740x555
7	351.085	685x514

Percobaan dilakukan sebanyak 2 kali dengan mengambil nilai *k=2* dan nilai *k=4*. Gambar rahasia yang digunakan adalah gambar berlatar belakang putih yang berisi tulisan. Gambar rahasia yang akan dienkripsi adalah sebagai berikut:



Proposal Makalah

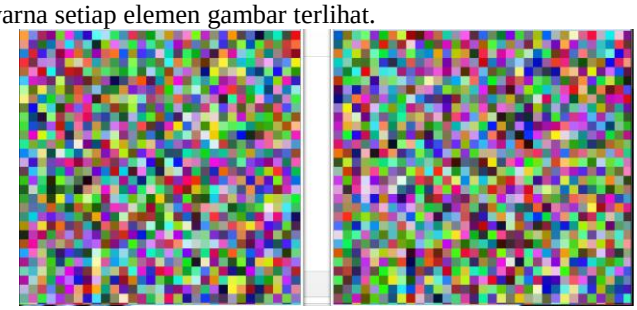
Proposal Makalah IF4020 Kriptografi

Judul Makalah : Kriptografi Visual Menggunakan Algoritma Berbasiskan XOR pada LSB Dua Buah Gambar Berbeda.
Nama : Yusuf Rahmatullah
NIM: 13512040

Gambaran Makalah
Kriptografi visual biasanya memecah secrete image menjadi dua buah share-image yang gambarnya tidak jelas (contoh pada gambar di bawah ini). Makalah ini menjelaskan mengenai kriptografi visual dari suatu secret-image yang menghasilkan dua buah gambar berbeda. Skema kriptografi visual yang digunakan dalam makalah ini berbasiskan XOR (penjelesan skema pada gambar di bawah ini). Share-image pada Gambar 1 menghasilkan dua gambar noise. Hal ini mudah dicurigai oleh orang lain. Hasil pemecahan secret-image disisipkan ke dalam LSB setiap gambar. Hal ini untuk mendistribusikan secret-image ke dalam dua gambar share-image yang berbeda sehingga tidak ada orang yang curiga mengenai gambar tersebut. Rekontruksi gambar menggunakan input kedua share-image.
Gambar 1 Kriptografi Visual Menggunakan Skema Kriptografi Berbasiskan XOR
Gambar 2 Skema Kriptografi Berbasiskan XOR
Bahan Referensi
Mostaghim, M., & Boostani, R. (2014). CVC : Chaotoc Visual Cryptography to Enhance Steganography. IEEE Conference Publications, 44-48.

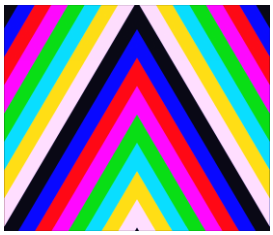
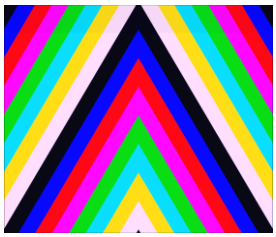
Hasil pembentukan gambar acak menghasilkan dua gambar seperti berikut ini

Hasil pembentukan gambar acak menghasilkan dua gambar seperti di bawah ini. Gambar telah diperbesar agar perbedaan warna setiap elemen gambar terlihat.

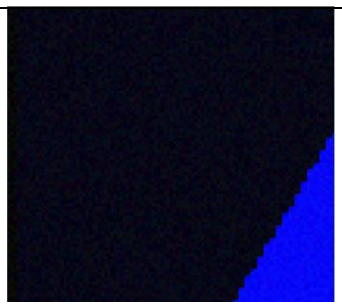


Kedua gambar di atas kemudian dimasukkan ke dalam dua gambar sampul. Gambar sampul yang digunakan berukuran 1280x960 dengan kedalaman warna 24-bit. Gambar sampul yang digunakan adalah gambar di bawah ini:

Hasil gambar sampul yang telah disisipi gambar acak dengan nilai *k=2* (gambar sebelah kiri) dan *k=4* (gambar sebelah kanan) adalah sebagai berikut:

Nilai PSNR masing-masing gambar sampul yang telah disisipi dengan gambar acak dengan nilai *k=2* dan *k=4* adalah 16,338 dB dan 22,165 dB. Gambar sampul yang telah disisipi gambar acak dengan nilai *k=4* memiliki kumpulan *noise* berupa bayangan hitam pada bagian atas gambar. Jika gambar diperbesar, maka perbandingan gambar sampul asli dengan gambar sampul yang telah disisipi gambar acak adalah sebagai berikut:

Gambar sampu asli	
k=2	
k=4	

V. KESIMPULAN DAN SARAN

Nilai PSNR gambar sampul yang telah disisipi gambar acak dengan masing-masing nilai *k=2* dan *k=4* masih di bawah 30dB. Hal ini menunjukkan bahwa metode yang dilakukan menurunkan kualitas gambar sampul. Hasil penyisipan gambar acak ke dalam gambar sampul dengan nilai *k=4* terdapat bayangan gelap berupa kumpulan *noise*. Jika gambar sampul diperbesar, *noise* akan terlihat jelas. Hal ini dapat menimbulkan kecurigaan orang ketiga. Oleh karena itu, nilai *k* yang aman untuk metode ini adalah *k=2*.

Kumpulan *noise* dapat dihilangkan dengan cara mengubah proses penyisipan. Penyisipan *k*-bit elemen gambar acak dapat disimpan pada sembarang koordinat unik dalam gambar sampul sehingga *noise* tersebar ke seluruh gambar sampul. Penyebaran *noise* membutuhkan proses tambahan untuk memeriksa apakah elemen gambar sudah pernah disisipi atau belum.

Penelitian lebih lanjut untuk meningkatkan nilai PSNR dapat dilakukan dengan melakukan perbaikan seperti memperbaiki algoritma pembangkitan gambar acak agar dihasilkan gambar acak yang memiliki perbedaan nilai warna yang relatif kecil dibandingkan dengan warna pada gambar sampul.

DAFTAR PUSTAKA

Ateniese, G., C. Blundo, A., & D. R. Stinson. (2001). Extended Capabilities for Visual Cryptography. *Theoretical Computer Science*, 143-161.

Mostaghim, M., & Boostani, R. (2014). CVC : Chaotoc Visual Cryptography to Enhance Steganography. *IEEE Conference Publications*, 44-48.

Munir, R. (2015). *Pengenalan Kriptografi Visual (Visual Cryptography).* Bandung: Teknik Informatika ITB.

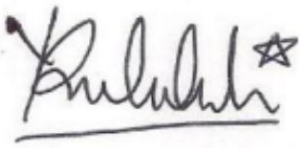
Naor, M., & A. Shamir. (1995). Visual Cryptography, Advances in Cryptology. *Eurocrypt '94 Proceeding LNCS*, 1-12.

Verheul, E. R., & H. C. A. van Tilborg. (1997). Constructions and Properties of K Out of N Vsual Secret Sharing Scheme. *Design Codes and Cryptography*, 179-196.

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, 10 Mei 2015



Yusuf Rahmatullah
13512040