Kriptografi Visual Biner dengan Skema(2,3) Ukuran 3x3 per *Pixel*

Zulhendra Valiant Janir (13510045)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510045@std.stei.itb.ac.id

***Abstract*—Kriptografi adalah salah satu metode penyembunyian atau penyamaran suatu pesan yang bersifat privat sehingga pesan menjadi tersembunyi maknanya. Kriptografi mengubah suatu pesan menjadi sesuatu yang tidak bisa dibaca oleh pihak yang tidak berkepentingan atau tidak berhak untuk membacanya. Fungsi kontrolnya terdapat pada peran kunci pada kriptografi.**

Kriptografi visual adalah suatu cara pengkodean sehingga dekripsi pesan bisa dilakukan hanya dengan indera penglihatan manusia tanpa perlu menggunakan bantuan komputer. Pada makalah ini, tipe kriptografi visual dengan warna biner atau hitam-putih dengan menggunakan skema(2,3) yang akan menghasilkan 3 *share* dengan kebutuhan *retrieval* 2 *share*. Dalam *generator*nya akan ada pembesaran ukuran 1x1 *pixel* menjadi 3x3.

***Index Terms*—Kriptografi visual, *share*, *pixel*.**

I. PENDAHULUAN

Pada zaman teknologi saat ini, sudah banyak komunikasi yang menggunakan media teknologi pada komunikasi langsung maupun tidak langsung. Semakin banyak kebutuhan dalam berkomunikasi, semakin tinggi permintaan kelengkapan spek atau fitur pada alat komunikasi tersebut. Salah satu fungsi yang dibutuhkan saat ini adalah keamanan agar privasi informasi dapat terpenuhi.

Dalam kegiatan penting seperti transaksi bisnis, mengurus kriminal, penyimpanan barang berharga, dan data rahasia pribadi membutuhkan keamanan agar tidak merugikan pihak yang berhak untuk mengetahui dan memiliki informasi tersebut. Walaupun informasi atau data tersebut tidak ditujukan kepada pihak lain, ada kemungkinan data tersebut dapat tersebar dan dilihat dengan bebas tanpa sepengetahuan pemilik yang kemudian mengakibatkan kebocoran informasi. Salah satu penyebabnya adalah lemahnya keamanan, metode, algoritma, virus, atau serangan dari pihak lain. Ada pun untuk berkomunikasi dengan pihak lain tanpa tersadap pihak ketiga, kedua pihak yang berkebutuhan untuk berkomunikasi dapat melakukan perjanjian dalam menggunakan kode atau simbol yang hanya diketahui oleh kedua belah pihak yang disampaikan secara bertatap muka atau metode komunikasi lainnya yang memiliki kemungkinan kecil untuk diketahui oleh pihak yang tidak berhak untuk mengetahuinya. Namun dengan komunikasi dengan metode yang minim akan penggunaan algoritma rumit serta kunci yang mudah diterka, metode ini hanya akan bertahan sebentar karena makna pesan sesungguhnya dapat ditebak dari pola yang ada dengan mempelajari banyak contoh dari pesan yang telah diubah menjadi kode. Kondisi ini dikarenakan sedikitnya simbol atau karakter yang digunakan dan persepsi umum pada masyarakat terhadap representasi simbol.

Dengan mempertimbangkan hal di atas, ada baiknya pemenuhan kebutuhan keamanan dalam berkomunikasi atau menyimpan informasi dengan teknik kriptografi algoritma baru serumit mungkin. Konsep yang diterapkan pada algoritma baru ini adalah mengubah gambar atau teks yang diubah menjadi gambar menjadi gambar biner (hitam-putih) yang kemudian dibuat menjadi gambar dengan ukuran yang lebih besar.

Ada pun pemenuhan kebutuhan umum dalam algoritma kriptografi dikelompokkan menjadi 4, yaitu:

1. *Confidentiality*

   Confidentiality mengharuskan pesan terenkripsi harus serancu mungkin sehingga susah untuk ditebak makna aslinya. Jika kriptanalisis memiliki banyak referensi algoritma, maka kriptanalisis tersebut dapat dengan mudah menerka algoritma yang digunakan maupun kuncinya. Sebisa mungkin algoritma yang digunakan adalah algoritma yang rumit dengan *range* kunci sebesar mungkin sehingga kriptanalisis membutuhkan pengorbanan berupa waktu dan tenaga sebesar mungkin.
2. *Authentication*

   Authentication menyediakan informasi tersirat mengenai identifikasi pengirim pesan. Hal ini dibutuhkan karena pada pengiriman pesan dapat terjadi pengakuan pengiriman pesan dari pengirim yang salah sehingga dapat merusak jalur komunikasi serta pembocoran informasi dengan adanya pihak yang seharusnya tidak berhak untuk terlibat atau sekedar mengetahuinya. Salah satu solusinya adalah dengan menggunakan kunci yang

sama pada pihak tertentu saja sehingga kedua pihak yang berkomunikasi mengetahui pengirim dan penerima pesan saat itu dari informasi yang diterima dan dikirim oleh masing-masing pihak.

3. *Integrity*

   Jika pihak yang tidak berhak untuk membaca atau menerima suatu pesan enkripsi tidak dapat mengerti arti dalam pesan tersebut, maka ada kemungkinan baginya untuk mengubah bahkan menghancurkan pesan tersebut sehingga arti yang sesungguhnya rusak ketika sampai pada penerima atau bahkan penerima tidak dapat menerima pesan sama sekali. Jika pesan yang terenkripsi diubah dan hasil dekripsinya tidak rusak atau masih bermakna, maka hal ini dapat merugikan penerima karena pesan asli berhasil diubah maknanya sehingga makna dari pesan asli tidak dapat diketahui. Selain itu jika penerima menerima pesan terdekripsi yang terubah tapi tidak mencurigakan, maka hal ini dapat merusak kepercayaan dari masing-masing pihak, tentunya hal seperti ini jarang terjadi mengingat susahnya untuk melakukan pengubahan tanpa cacat atau kecurigaan. Sebaiknya algoritma enkripsi yang digunakan dapat mendeteksi perubahan sekecil mungkin pada pesan enkripsi yang telah diubah.

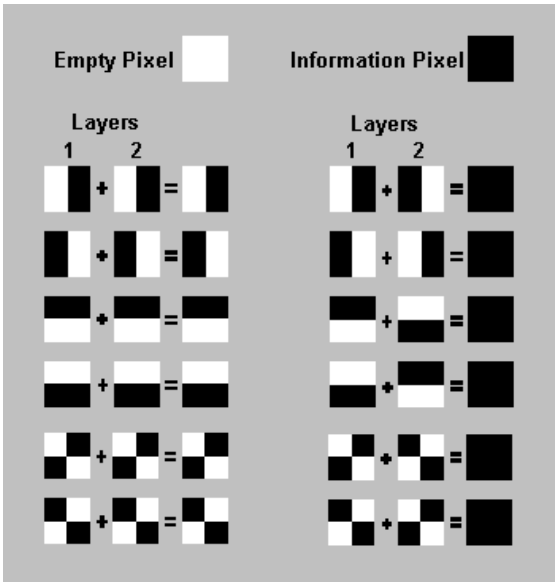
4. *Nonrepudiation*

   Demi suatu kepentingan atau manipulasi di luar penerapan kriptografi, pengirim pesan dapat menyangkal bahwa dia telah mengirim pesan tertentu dengan cara mengubah kembali hasil enkripsi pesannya. Cara mengatasinya adalah dengan cara membuat deteksi perubahan hasil enkripsi dengan menyimpan data pesan asli pada proses enkripsi sehingga nantinya dalam proses dekripsi dapat dilakukan verifikasi.

Kriptografi visual sendiri merupakan teknik kriptografi menggunakan gambar dengan pola yang unik. Ada pun dekripsinya dapat dilakukan dengan menggunakan penglihatan manusia tanpa menggunakan komputer.

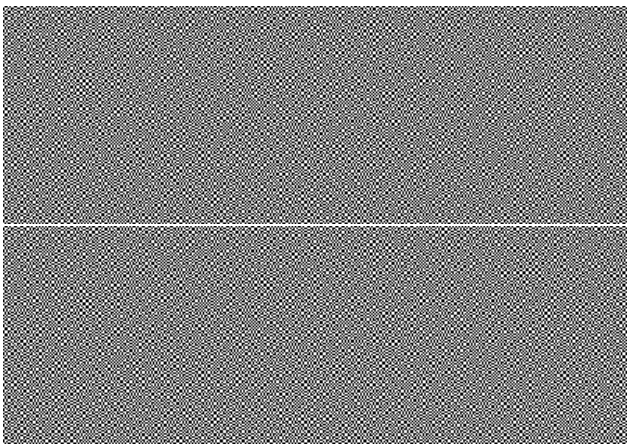
Kriptografi visual dikembangkan pertama kali oleh Moni Naor dan Adi Shamir pada sekitar tahun 1994 pada jurnal *Eurocrypt*. Dengan menggunakan skema(k,n) *sharing* visual rahasia yang gambarnya dipecah menjadi n bagian sehingga hanya seseorang yang memiliki minimal k bagian tersebut yang bisa mendeskripsi gambar. Jika kurang 1 gambar saja, maka gambar tidak akan menghasilkan dekripsi yang memuaskan. Namun nilai k sebaiknya lebih kecil sama dengan n dan lebih besar dari 1.

Metode enkripsi kriptografi visual adalah dengan membagi pesan asli sehingga memiliki partisi gambar yang berbeda. Untuk memastikan gambar sedetil mungkin, gambar pesan diperbesar x kali lipat tergantung pembagian 1 *pixel* terhadap n x n *pixel*. Berikut adalah konsep pembagian tiap 1 *pixel* menjadi beberapa *share* dalam ukuran 2x2.



Gambar 1 Pembagian 1 *pixel* menjadi 4 *pixel*

Sedangkan metode dekripsi kriptografi visual hanya perlu menumpuk *share* seperlunya dari pesan terenkripsi. Ketika semua gambarnya ditumpuk, maka gambar aslinya akan terlihat.



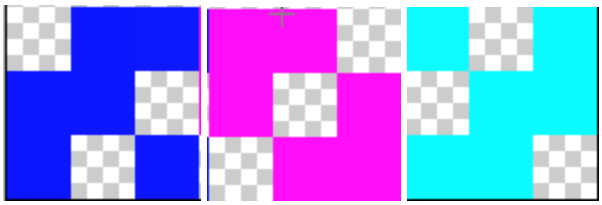
Gambar 2 *Share* hasil enkripsi

Gambar 3 Tumpukan kedua *share* pada Gambar 2

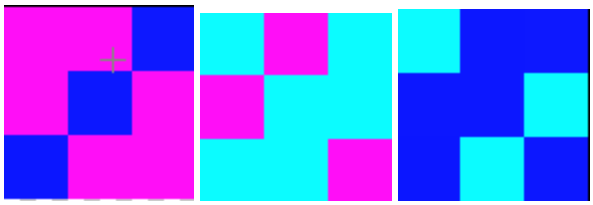
II. METODE

Berdasarkan alur dari kriptografi visual dan untuk keamanannya, maka enkripsi dilakukan oleh pihak ketiga yang terpercaya atau disebut sebagai *dealer*. Lalu hasilnya yang berupa *share* akan diberikan pada partisipan dan kemudian didekripsi dengan cara menumpuk citra yang dicetak pada plastik transparan.

Metode yang digunakan kali ini mempunyai beberapa batasan dan aturan, yaitu gambar pesan merupakan citra biner, ukuran *share* diperbesar n kali, skema yang digunakan adalah(k,n) dengan k adalah 2 dan n adalah 3. Dengan mengubah 1x1 *pixel* menjadi ukuran 3x3, maka didapat 3 share yang saling melengkapi.



Gambar 4 Tiga macam *pixel share*, 0 (kiri), 1 (tengah), 2 (kanan)



Gambar 5 Gabungan dari dua *pixel share* yang komplemen

Ketiga share pada Gambar 4 tersebut dikodekan sebagai *pixel* 0, 1, dan 2 secara berurutan.

A. Enkripsi

1. Tahap Penyediaan Pesan

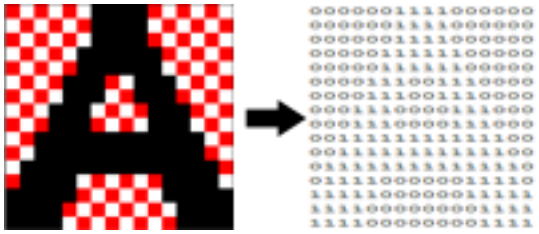
   Untuk membuat teks menjadi gambar, maka dibutuhkan template gambar yang memadai. Berikut adalah salah satu *website* yang menyediakan aplikasi untuk membuat gambar dari teks dengan cepat, fungsional, dan mudah http://interactimage.com/ .

   Setelah gambar pesan didapat, selanjutnya citra yang diproses diubah menjadi citra biner jika gambar pesan awalnya merupakan citra fullcolor atau grayscale. Metode ini dapat dilakukan manual dengan menggunakan aplikasi Adobe Photoshop.

Gambar 6 Mode gambar

2. Tahap Pemetaan

   Pada tahap ini, informasi dari gambar akan dipetakan menjadi matriks dengan domain biner, 0 dan 1 di mana 1 artinya terdapat informasi atau citra yang memiliki *pixel* hitam dan 0 artinya tidak ada informasi pada suatu koordinat titik.

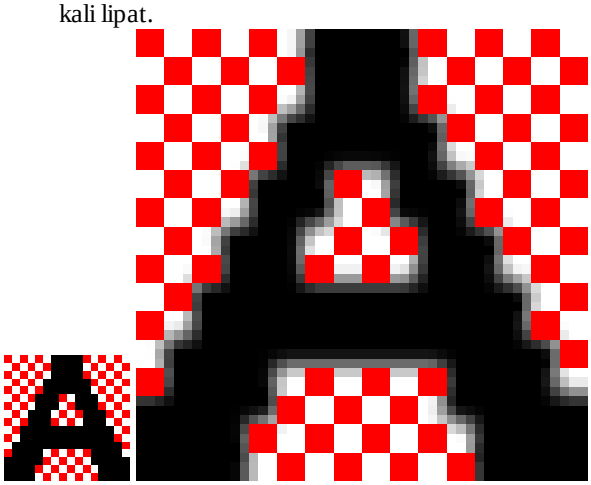


Gambar 7 Pemetaan matriks

Dari proses tersebut didapatkan informasi biner pada matriks serta luas bidang pada citra.

3. Tahap Pembesaran

   Untuk meningkatkan akurasi dekripsi gambar, pembesaran butuh dilakukan tergantung pembagian *pixel* yang digunakan. Untuk pembagian 3x3 maka pembesaran dilakukan 9 kali lipat dengan lebar dan panjang masing-masing 3 kali lipat.



Gambar 8 Pembesaran huruf A

4. Tahap Enkripsi dan Penyediaan *Background*

   Yang dimaksud dengan *background* adalah pola-pola *pixel* berukuran 3x3 yang bukan merupakan *pixel* hitam yang nantinya akan diisi citra pesan.

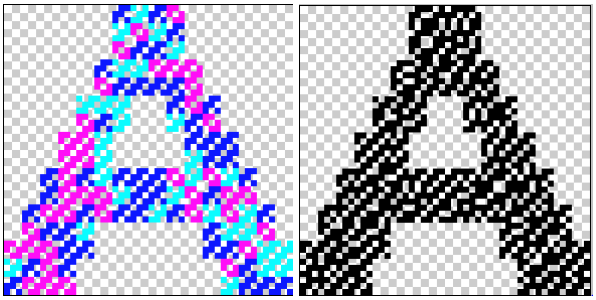
   Pola background akan beragam tergantung kunci yang digunakan serta space yang digunakan. Berikut adalah algoritma yang digunakan.

```
public void Random(int x, int y, int A){
        int a=0;
        int x0=0;int x1=0;int x2=0;

        for(int i=0;i<A;i++){
            r=(i+y+a)%x;
            a=(i+y+a)%3;

            if(a==0)
                x0++;
            else if(a==1)
                x1++;
            else
                x2++;
        }
}
```

Gambar 9 Source code algoritma pembangkit urutan *pixel share*

Dengan x dan y adalah sepasang kunci dan A merupakan luas pixel. x0,x1,x2 adalah jumlah kemunculan angka 0, 1, dan 2 oleh pembangkit dengan variabel a.

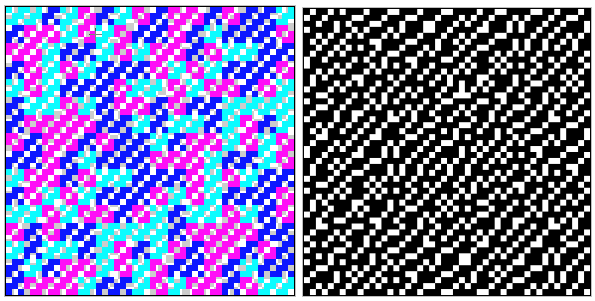
Setelah melakukan percobaan terhadap x dan y, ditemukan kunci yang persebarannya cukup bias (untuk A=10000, maka x0 = 4102, x1 = 3460, x2 = 2438), yaitu x = 13 dan y = 19 dengan perulangan pola setiap 68 *pixel* 3x3. Kunci ini digunakan untuk barisan matriks yang hanya bernilai 1 secara berurut baris lalu kolom. Berikut adalah hasil dari penggunaan kunci serta implementasinya.



Gambar 10 Hasil implementasi *share* 1 dengan modifikasi warna (kiri) dan hasil akhir biner (kanan)

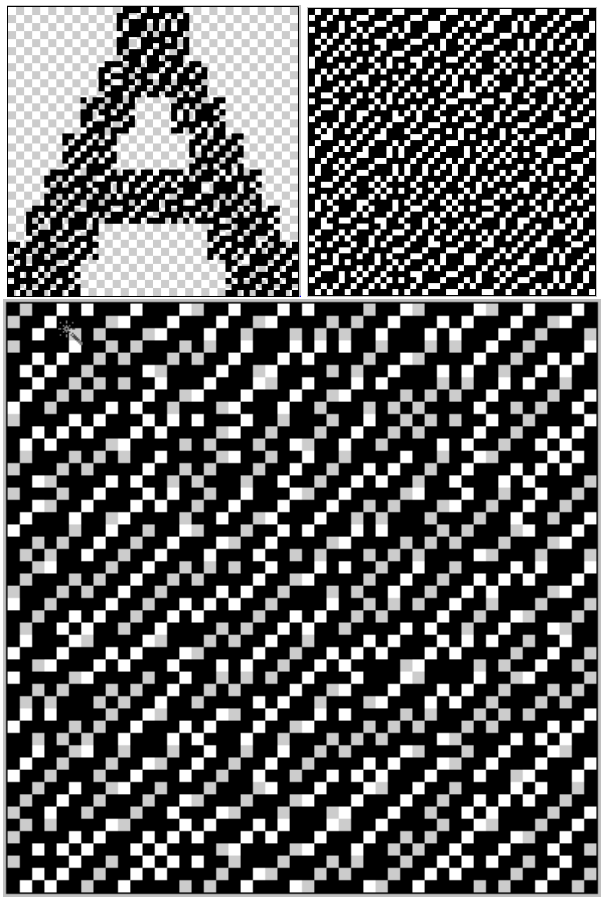
Untuk *share* 2 hanya dengan mengubah kode pixel = (kode pixel + 1) mod 3. Dan seterusnya untuk *share-share* berikutnya.

Agar algoritma dapat diperkuat, dibuat juga sebuah kunci berbeda untuk pembuatan background. Ditemukan kunci bias lainnya (untuk A=10000, maka x0 = 3619, x1 = 3429, x2 = 2952), yaitu x = 7 dan y = 23 dengan perulangan pola setiap 105 *pixel* 3x3. Kunci ini digunakan untuk barisan matriks yang bernilai 1 maupun 0 secara berurut baris lalu kolom. Berikut adalah hasil dari penggunaan kunci serta implementasinya.



Gambar 11 Hasil implementasi *background* dengan modifikasi warna (kiri) dan hasil akhir biner (kanan)

Selanjutnya adalah melakukan *overlapping* dari tiap *share* terhadap background, berikut adalah hasilnya dengan cara penumpukan.



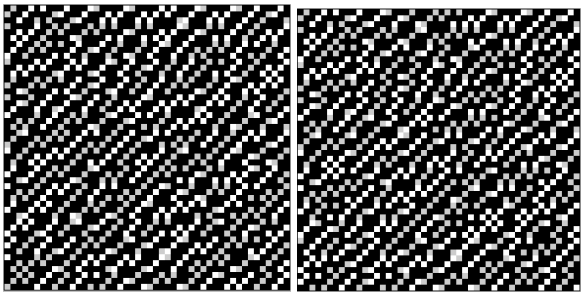
Gambar 12 Hasil Penyatuan (bawah) dan sumber penyatuan (atas)

Dilakukan hal yang serupa untuk *share-share* berikutnya pula. Akhirnya, semua *share* pun jadi dan tinggal digunakan.

B. Dekripsi

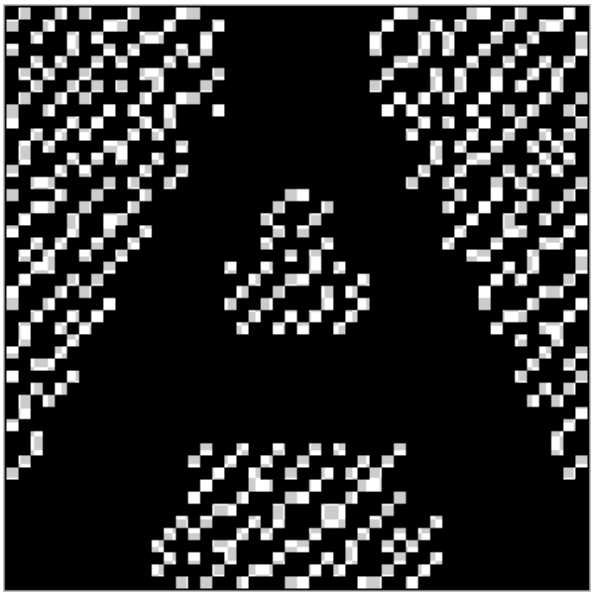
1. Penumpukan

   Tentunya untuk mengembalikan pesan bermakna dari citra terenkripsi, dibutuhkan minimal 2 share yang dibutuhkan.



Gambar 13 *Share* 2 (kiri) dan *share* 3 (kanan)

Selanjutnya dapat dilihat hasil penumpukan dari minimal 2 *share*. Berikut adalah salah satu penumpukan, tidak ditampilkan ketiga kemungkinan karena menghasilkan gambar dekripsi yang sama.



Gambar 14 Hasil penumpukan minimal 2 *share*

2. Pembacaan Pesan

   Pesan terenkripsi yang sudah ditumpuk akan menghasilkan gambar yang sekiranya jelas. Namun gambar yang muncul bukanlah gambar asli yang sama dengan gambar yang belum dienkripsi. Dalam percobaan ini, pesan dalam gambar dapat terlihat dengan jelas, yaitu pesan berupa teks atau sebuah huruf 'A'.

III. Analisis

Dari hasil percobaan dengan menggunakan algortima kriptografi visual, gambar yang dihasilkan dapat beragam tergantung kuncinya. Namun jika kunci yang digunakan menghasilkan *pseudo random* yang lemah, maka akan menyebabkan terbentuknya pola pada gambar sehingga proses pengembalian *share* menjadi gambar asli akan mudah tanpa harus memiliki semua *share*.

Pola persebaran kunci akan lebih baik jika kunci merupakan bilangan prima dan sebaik mungkin menghindari kelipatan n atau dalam percobaan ini adalah 3.

Karena satu *pixel* gambar asli merepresentasikan 9 *pixel* atau 3x3, maka *share* mudah diketahui keterkaitannya dengan jumlah *pixel* pembesaran.

Sebagai penerapan algoritma kriptografi visual, tentunya pesan akan mudah untuk didekripsi siapapun tanpa perlu menggunakan komputer jika memiliki *share* yang cukup. Ini menyebabkan mudahnya metode kriptanalisis, yaitu dengan memiliki *share* berbeda sebanyak-banyaknya. Ada pun metode lain yang sangat rumit yaitu dengan menganalisis pola pada tiap *share* untuk mendapatkan kuncinya, biasanya kondisi ini digunakan ketika kriptanalisis tidak mempunyai cukup banyak share.

Jika background tiap share adalah sama, maka untuk skema(n,n) dengan n lebih besar dari 10 dengan mendapatkan 2 *share*, kriptanalisis bisa menemukan pola di mana *pixel* informasi terdapat pada alur grafis yang berubah sejak penumpukan.

IV. Kesimpulan

Metode yang dipakai merupakan metode yang tidak mapan sehingga tidak cocok untuk citra *fullcolor* dan *grayscale*. Dan karena adanya pembesaran dari gambar pesan menjadi sejumlah *share*, hal ini menyebabkan *oversized* ketika pengiriman gambar sehingga membutuhkan media pengiriman yang lebih mapan pula karena ukuran yang dikirimkan 9 kali lebih besar. Kriptanalisis pun mudah untuk menemukan pola gambar jika algoritmanya tidak cukup aman.

IV. Daftar Gambar

REFERENSI

[1] Munir, Rinaldi. 2005. *Diktat Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika, Institut Teknologi Bandung.
[2] http://interactimage.com/ (18.10, 19 Mei 2013)
[3] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah2/Makalah2-IF3058-Sem2-2010-2011-013.pdf (20.13, 6 Mei 2013)
[4] http://www.cs.nccu.edu.tw/~raylin/UndergraduateCourse/ComtenporaryCryptography/Spring2009/VisualCrypto.pdf (18.32, 19 Mei 2013)

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

Zulhendra Valiant Janir (13510045)