Kriptografi Visual Berwarna dengan Metode Expansi Halftone

Everaldo Sembiring(13510095)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13510095@std.stei.itb.ac.id

Abstrak

Melalui makalah ini akan dijelaskan salah satu metode kriptografi visual yaitu metode expansi halftone.Dengan menggunakan metode ini akan dihasilkan dua buah share yang dibutuhkan untuk dapat membentuk image yang asli.

Pada bagian akhir makalah ini akan dijelaskan juga pendapat penulis mengenai potensi perkembangan kriptografi visual di dalam dunia kriptografi.

***Index Terms*—Kritografi visual,*halftone color,image share,PSNR*.**

I. PENDAHULUAN

Pada zaman ini sudah menjadi hal biasa setiap orang bertukar file multimedia melalui internet.Sehingga dibutuhkan solusi agar file tersebut tetap aman ketika berada di internet.Salah satu hal yang dapat diterapkan adalah dengan menggunakan metode kriptografi yang memerlukan kunci untuk bisa membuka file tersebut.Namun kekurangannya,dibutuhkan komputasi untuk dapat membuka file tersebut.

Pada tahun 1994,Naor dan Shamir menemukan cara untuk dekripsi citra tanpa harus menggunakan kunci serta komputasi.Caranya adalah dengan membagi sebuah gambar menjadi beberapa share yang terenkripsi.Agar gambar tersebut dapat dilihat kembali,diperlukan t share dari n share.Sehingga apabila hanya memilki lebih kecil dari t share,maka tidak dapat diketahui gambar aslinya.

Namun,penemuan dari Naor dan Shamir masih terbatas pada gambar *grayscale* saja,kurang baik jika diimplementasikan pada gambar yang bewarna.Dari dulu juga sudah banyak penelitian yang pernah dilakukan mengenai visual kritografi.Namun kebanyakan tetap mendiskusikan bagaimana merahasiakan gambar bewarna hitam dan putih saja.Padahal pada masa kini yang diperlukan adalah bagaimana untuk mengamankan citra yang bewarna.

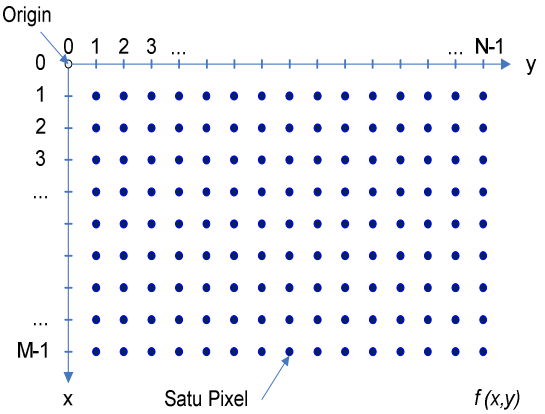
Melalui makalah ini,penulis akan menjelaskan salah satu metode yang dapat digunakan dalam merahasiakan citra yang bewarna.Metode yang digunakan mengembangkan metode yang telah digunakan oleh Naor dan Shamir.Detail dari metode ini akan dijelaskan pada bagian –bagian berikutnya.

II. TEORI DASAR

II.1.Citra(*image*)

Citra dalam komputer adalah sekumpulan pixel-pixel yang disusun membentuk sebuah gambar yang dapat dilihat oleh pengguna.

Setiap pixel yang membangun sebuah citra tediri atas tiga gabungan warna dasar.Di dalam komputer,warnatersebut dikenal sebagai *RGB*(*Red,Green,Blue*).



Gambar 1:Representasi Citra

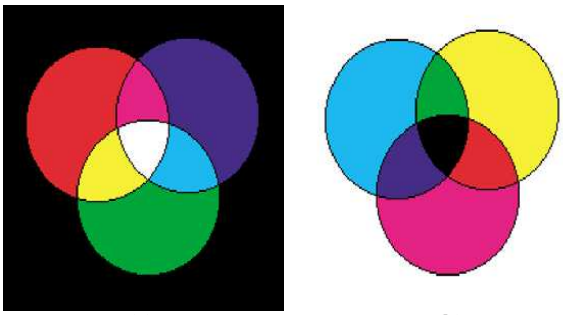
II.2.Warna

Seperti disebutkan sebelumnya,warna primer tersusun atas warna merah,hijau,dan biru.Warna lain dapat diperoleh dengan menggabungkan ketiga warna tersebut.Contohnya,warna putih dapat diperoleh dengan menggabungkan ketiganya.

Representasi warna memiliki dua model:*additive* dan *subtractive*.Model *additive* berlaku jika komposisi ketiga warna tersebut semakin banyak,maka hasilnya akan semakin terang.Model *subtractive* adalah warna cahaya yang dipantulkan dari sebuah objek.Jika sebuah cahaya menabrak sebuh objek,tidak seluruh cahaya akan dipantulkan.Sebagian akan diserap,sebagian dipantulakan.Dengan menggabungkan warna *Cyan* (C) dengan Magenta (M) dan kuning (Y),dapat dihasilkan warna lainnya.Semakin besar komposisinya,maka akan semakin gelap.Demikian sebaliknya akan menghasilkan warna terang.

Karena dalam kriptografi visual menghasilkan gambar yang bersifat transparan,maka model *subtractive* cocok digunakan.RGB dan CMY adalah warna yang saling berlawanan.Dengan demikian untuk mencari CMY dari RGB adalah sebagai berikut:

C=255-R,M=255-G,Y=255-B



(a) (b)

Gambar 2: (a) Model Additive; (b) Model subtractive.

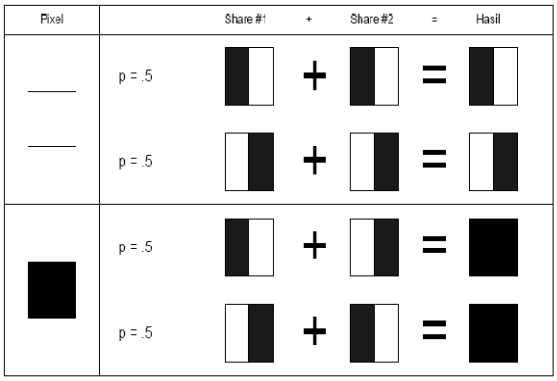
Gabungan warna pada CMY juga komplementer dari gabungan warna RGB.Berikut adalah tabel kombinasi warna pada CMY:

Warna	Representasi (C, M, Y)
White	{0, 0, 0}
Cyan	{1, 0, 0}
Magenta	{0, 1, 0}
Yellow	{0, 0, 1}
Purple	{1, 1, 0}
Orange	{0, 1, 1}
Green	{1, 0, 1}
Black	{1, 1, 1}

Tabel 1:Kombinasi warna CMY

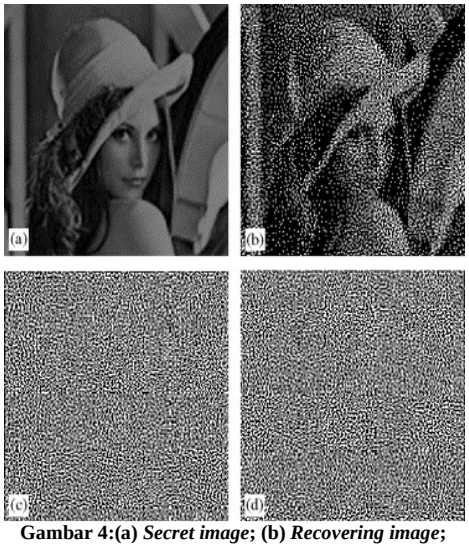
II.3.Kriptografi Visual

Kriptgrafi visual pertama kali dikembangkan pertama kali oleh Naor dan Shamir padagambar hitam dan putih.Model yang mereka gunakan adalah dengan membagi sebuh pixel menjadi m sub-pixel.



Gambar 3:Model pixel Naor dan Shamir

Pada metode ini akan dihasilkan dua buah share.Dari sebuah pixel akan dipilih satu dari dua kemungkinan kombinasi share.Kemudian dua share digabungkan: hitam dan hitam menjadi hitam,hitam dan putih menjadi hitam,putih dan putih menjadi putih.Pixel bewarna putih tidak menghasilkan warna putih namun gabungan antara warna putih dan hitam.Sehingga gambar asli akan terdegradasi sebesar 50%.Meskipun terdegradasi sebesar itu,gambar tersebut masih dapat dimengerti oleh mata manusia.



Gambar 4:(a) *Secret image*; (b) *Recovering image*; (c) *Share image* 1; (d) *Share image* 2.

Secara umum,kriptografi visual memiliki kelemahan sebagai berikut:

- Citra hasil dekripsi tidak tepat sama dengan citra asli.
- Citra hasil dekripsi mengandung *noise*.
- *Share* tidak memiliki makna sehingga dapat menimbulkan kecurigaan bahwa gambar tsb merupakan pesan rahasia.

Untuk mengurangi kelemahan tersebut,dilakukan banyak penelitian dengan mengubah parameter-parameter yang ada.Setiap metode memiliki kekurangan dan kelebihannya masing-masing.Berikut adalah penemuan-penemuan kriptografi visual yang ada:

Penemu	Jumlah Share	Jumlah sub-pixel	Format Citra	Tipe share yang dihasilkan
Naor dan Shamir	1	4	Binary	Acak
Wu dan Chen	2	4	Binary	Acak
Hsu et al	2	4	Binary	Acak
Wu dan Chang	2	4	Binary	Acak
Chin-Chen Chang et al	1	4	Binary	Bermakna
Liguo Fang et al	1	2	Binary	Acak
S. J. Shyu et al	n(n>=2)	2n	Binary	Acak
W. P. Fang	2	9	Binary	Acak
Jen-Bang Fenget al	n(n>=2)	3n	Binary	Acak

Mustafa Ulutas	2	4	Binary	Acak
Tzung-Her Chen et al in	2	1	Binary	Acak
Tzung-Her Chen et al	n(n>=2)	4	Binary, *grey* color, bewarna	Acak
Wen-Pinn Fang	2	1	Binary	Acak
Zhengxin Fu	4	9	Binary	Acak
Jonathan Weir et al	n	4	Binary	Acak
Xiao-qing Tan	1	1	Binary	Acak
Verheul Tilborg	1	C*3	Bewarna	Acak
Yang & Liah	1	C*3	Bewarna	Acak
Chang and Tsai	1	529	Bewarna	Bermakna
Chin Chen Chang et al	1	9	*Gray*	Bermakna
Lukac and Plataniotis	1	2	Bewarna	Acak
R.Youmaran et al	1	9	Bewarna	Bermakna
S.J.Shyu	1	$[\text{Log}_2$ c*m]	Bewarna	Acak
Mohsen Heidarinejad et al	1	9/16	Bewarna	Acak
Haibo Zhang et al	1	1	*Gray*	Acak
F. Liu et al	1	1	Bewarna	Acak
Wei Qiao et al	1	m	Bewarna	Acak
Du-Shiau Tsai et al	1	9	Bewarna	Bermakna

Tabel 2:Komparasi skemakriptografi visual

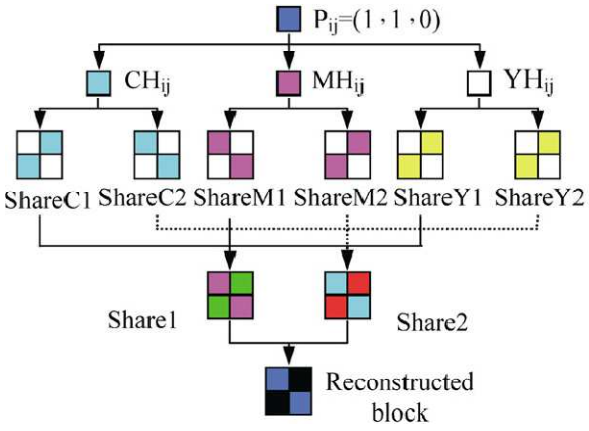
Dari tabel di atas dapat dilihat perbedaannya.Terdapat metode yang meminimalkan jumlah sub-pixel.Metode ini cocok untuk mengtransmisikan citra pada bandwith yang terbatas.Untuk dapat menghindari serangan dari hacker,terdapat juga metode yang dapat menghasilkan share yang bermakna.

Pada makalah ini,akan difokuskan pada secret image yang bewarna karena pada saat ini file yang ditransmisikan adalah file pada lingkungan multimedia.Salah satunya dengan Extended Halftone.

III.Extended Halftone

III.Metode

Metode ini akan menghasilkan dua buah share.Caranya adalah dengan mengtransformasi blok-blok RGB menjadi CMY. Satu buah pixel ditransformasi menjadi 2x2 sub-pixel.Kemudian,dengan metode yang mirip pada metode Naor dan Shamir,setiap pixel menghasilkan dua buah sub-share.Jika pixel bernilai 0(putih),maka sub-share yang dihasilkan akan saling berlawanan.Jika bernilai 1,maka kedua sub-share akan bewarna sama.Sehingga akan terdapat 6 buah sub-share C1,C2,M1,M2,Y1,Y2.setiap share pasti akan memilki ½ pixel bewarna putih dan ½ pixel bewarna C atau M atau Y.Share 1 diperoleh dengan menggabungkan setiap sub-share berindex satu:C1,M1,Y1.Sedangkan share 2 diperoleh dengan menggabungkan C2,M2,Y2.Kedua share inilah yang akan dikirimkan ke internet.



Gambar 5:Skema Metode Expansi Halftone

Seperti yang dilihat pada gambar di atas,warna CMY didefinisikan dengan 1 atau 0.Hal ini dilakukan dengan menggunakan threshold.Jika nilai warna melebihi threshold maka warna tersebut bernilai 1,selain itu 0(transparan).Contohnya jika komposisi warna CMY : (50,170,200) dengan threshold 150,maka P_{ij} yang dihasilkan adalah (0,1,1).

III.2.Algoritma

1. Transformasikan citra asli menjadi tiga gambar:*Cyan*,*Magenta*,dan *Yellow*.
2. Untuk setiap pixel dilakukan langkah sebagai berikut:
   2.1.Dengan menggunakan metode Naor dan Shamir pada pixel bewarna hitam dan putih, setiap C_{ij},M_{ij},C_{ij} di-ekspansi menjadi blok 2x2: C_{1ij}, C_{2ij} ,M_{1ij} ,M_{2ij},Y_{1ij} ,Y_{2ij}.
   2.2.Gabungkan pixel pada C_{1ij}, M_{1ij} , Y_{1ij} untuk memperoleh P_{ij} share 1.
   2.2.Gabungkan pixel pada C_{2ij}, M_{2ij} , Y_{2ij} untuk memperoleh P_{ij} share 2.
3. Ulangi langkah kedua untuk setiap P_{ij} . Sehingga pada akhirnya akan diperoleh dua buah share yang dapat menghasilkan gambar rahasia.
4. Jika kedua gambar tersebut disatukan maka akan diperoleh gambar rahasia dapat dilihat oleh mata manusia.

IV. HASIL EXPERIMEN

Langkah awal dalam melakukan eksperimen adalah menentunkan threshold,berapakah nilai C,M, dan Y yang menyebebabkan expansi pixel bernilai satu.Pada awalnya penulis menetapkan nilai sebesar 100.Dari hasil pengujian beberapa objek,berikut salah satu kombinasi share dan hasil *stacking*-nya sebagai berikut:

(a) (b)

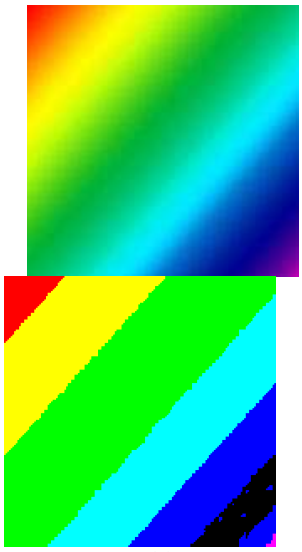
(c) (d)

Gambar 6:(a) *Secret image*; (b) *Recovering image*; (c) *Share image* 1; (d) *Share image* 2.

Ternyata hasil yang diperoleh cukup bagus walaupun sudah sangat terdegradasi.Walaupun gambar sudah tidak sempurna,makna gambar tersebut masih dapat dimengerti oleh manusia.

Gambar tersebut tergdegradasi dimungkinkan karena blok pixel yang dihasilkan memang tidak sempurna.Contohnya sebuah blok bewarna biru,jika direcovery akan memiliki kombilan 2/4 blok biru dan 2/4 blok hitam.Dalam gambar tersebut,setiap pixel direcovery menghasilkan 2 pixel bewarna hitam.Sehingga gambar menjadi lebih gelap.

Perbedaan juga akan lebih kelihatan jika algoritma diimplementasikan pada gambar warna gradasi.Komposisi warna gradasi menjadi tidak kelihatan.Setiap warna di perbatasan dua warna yang berbeda akan ditampilkan warna yang lebih dekat dengan putih saja.Contohnya antara hijau dan biru muda akan dihasilkan hijau karena hijau memang lebih dekat dekat warna putih.



(a) (b)

Gambar 7:(a) *Secret image*; (b) *Recovering image*;

Hal ini disebabkan karena atribut dari setiap warna antara 0 dan 1.Sehingga warna gradasi tidak mungkin dimasukkan kedalam algoritma ini.Kombinasi warna yang mungkin ada delapan warna saja.Apabila warna tersebut adalah warna gradasi maka hasil recovery adalah warna kencederungannya.Contohnya,warna biru gelap kencenderungannya adalah warna hitam,sehingga warna biru gelap ditransformasikan ke warna hitam.Hasilnya dapat dilihat pada gambar 7,gradasi warna biru terang dan biru gelap menjadi tidak sempurna.Warna biru gelap lebih cenderung hitum dibandingkan dengan warna aslinya.

Berdasarkan uji coba,ternyata threshold berpengaruh besar pada contrast dari *recovering image.*Berikut adalah perbandingan gambar pada threshold 100 dan 150:

Gambar 8:(kiri) *Recovering image dengan threshold 100*; (kanan) *Recovering image dengan threshold 150*;

Hal ini dikarenakan semakin tinggi threshold yang digunakan maka semakin banyak sedikit nilai 1 pada C,M,dan Y.Sehingga warna putih menjadi semakin dominan daripada warna aslinya.Sedangkan pada threshold 100,semakin banyak warna aslinya semakin banyak juga warna hitam yang dihasilkan.Akibatnya warna gambar akan menjadi semakin gelap.Threshold yang tinggi dan kecil memiliki kelebihan dan kekurangannya masing-masing.Namun dari hasil ujicoba,hasil dari dua jenis threshold tersebut terbukti masih dapat dilihat oleh mata manusia.

Dari hasil pengujian yang sudah dilakukan,hasil yang diperoleh cukup memuaskan.Dari penjelasan diatas maka ditemukan empat hal yang penting dari algoritma ini:

1. Kombinasi blok menentukan kesamaan tiap pixel antara *secret image* dengan *recovery image*,
2. Kombinasi warna berpengaruh pada warna gradasi,
3. Threshold mempengaruhi *contrast* dari *recovery image*.
4. Recovery image hanya dapat diperoleh jika memiliki kedua share.

Namun Algoritma ini masih kurang aman karena menghasilkan 2 share saja.Dengan jumlah share yang sedikit tentu lebih mudah juga untuk menemukan gambar yang dirahasikana.

Algoritma ini juga hanya cocok pada file berukuran kecil saja,yaitu jumlah pixelnya cukup kecil.Hal ini dikarenakan setiap secret image ukurannya menjadi dua kali lebih besar karena 1 pixel ditransformasikan menjadi 2x2 sub-pixel.Sehingga algoritma ini tidak cocok untuk mengtransmisikan file berukuran besar.

Dari sisi keamanan juga masih dapat menimbulkan kecurigaan karena tipe share yang dihasilkan masih berupa gambar acak.Oleh karena itu perlu dilakukan steganografi apabila tidak ingin menimbulkan kecurigaan penyerang.

Akan tetapi algoritma ini sudah cocok diterapkan pada citra bewarna.Hasil recovey image dapat dimengerti oleh mata manusia.Oleh karena itu algoritma ini sudah cukup untuk mengtransmisikan file rahasia namun tidak memerlukan tingkat keamanan yang tinggi.Tidak cocok untuk file seperti dokumen negara,keamanan militer,ataupun file yang memerlukan tingkat keamanan tinggi lainnya.

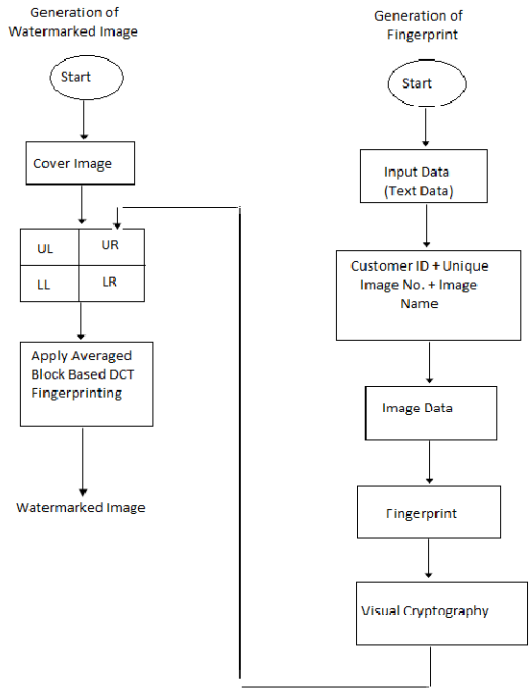
V. POTENSI KRIPTOGRAFI VISUAL KE DEPAN

Penyimpanan informasi dengan menggunakan kriptografi visual akan semakin banyak diterapkan nantinya karena kedepannya akan semaking banyak sekali pertukaran data melalui internet.Visual kriptografi unggul dengan memanfaatkan kemampuan visual manusia dibandingkan dengan algoritma lain yang membutuhkan komputasi.Algoritma kriptografi visual dapat dipergunakan dalam mengtransmisikan dokumen rahasia seperti:dokumen pertahanan,dokumen bisnis,dokumen negara,dan hal-hal lain yang harus dirahasiakan.

Salah satu penerapan kriptogragi visual terdapat pada autentikasi biometrik.Autentikasi biometrik menggunakan aspek fisik yang dimiliki oleh manusia seperti iris mata,sidik jari,retina,dan tekstur wajah.Sehingga hanya pengguna yang sama dapat terautentikasi oleh mesin.Namun jika data tidak dirahasiakan maka akan mudah diubah oleh penyerang.

Salah satu teknologi autentikasi biometric yang kita kenal adalah fingerprint.Dalam menggunakan fingerprint ternyata dibutuhkan juga kriptografi visual.Kegunaannya adalah menjaga kerahasiaan identitas yang ada dalam database fingerprint tersebut.Share yang dihasilkan kemudian di *watermark*, sehingga dapat dideteksi jika terjadi pengubahan pada share tersebut.Berikut adalah langkah jelasnya:

1.Mulai.
2.Dilakukan input informasi bertipe text yang berisi informasi seperti id,nama,dan informasi lainnya.
3.Informasi tersebut diubah menjadi sebuah gambar,kemudian gambar tersebut dibagi menjadi n share.
4.Dengan menggunakan salah satu metode watermark,maka informasi tersebut menjadi aman terhadap perubahan.
5.Informasi fingerprint dapat diakses dengan aman.



Gambar 9: Skema salah satu pemanfaatan kriptografi visual dalam menjaga database fingerprint.

Dalam dunia bisnis,kriptografi visual dapat menjadi hal penting.Dalam berbisnis,sangat tidak diharapkan metode keamanan yang kompleks dan lama untuk di-*decode*.Sedangkan kriptografi visual hanya membutuhkan visualisasi manusia.Namun kesulitan dalam menerapkan aplikasi ini dalam dunia bisnis adalah harus meminimalkan noise.Noise yang terlalu besar dapat menyebabkan dokumen menjadi sulit untuk dibaca sedangkan dokumen bisnis haruslah sangat jelas sehingga dokumen tersebut dapat dipercaya.

Semakin berkembangnya teknologi semakin banyak pula penipuan-penipuan dan pencurian informasi yang sering terjadi di internet.Salah satunya adalah dengan cara phishing.Metode pishing digunakan dengan menggunakan form yang diisi oleh pengguna.Form tersebut dapat berupa informasi nomor kartu kredit,nomor rekening,dan informasi sensitif lainnya.Namun pengguna tidak sadar

pada saat mengisi form tersebut.Visual kriptografi sangat bermanfaat untuk menjadi anti-phishing.Pada saat regristrasi,user diberikan sebuah secret image dan image tersebut dibagi menjadi dua buah share.Share pertama diberikan kepada user dan share kedua disimpan di server.Kemudian setiap kali memasuki situs,aplikasi akan meminta username,kemudian server meminta user memasukkan share yang dimilikinya.Server akan melakukan *stacking* share dari user dengan share dari server kemudian hasilnya ditampilkan ke user.Bila gambar yang dihasilkan benar maka user telah terhindar dari web pishing,jika tidak maka user dapat langsung keluar dari web tersebut.

VI. KESIMPULAN

Dengan berkembangnya teknologi,pertukaran informasi semakin tidak jarang dilakukan.Selain untuk pertukaran informasi dibutuhkan juga metode pengamanan untuk menjaga informasi yang bersifat sensitif.Pertukaran informasi pada masa kini lebih sering menggunakan file multimedia yang bewarna.

Metode Extended Halftone ini mencukupi untuk menjaga kerahasiaan pada citra yang bewarna.Namun masing kurang aman karena dapat menimbulkan kecurigaan bagi penyerang.Oleh karena itu penulis menyarankan agar metode ini disertai dengan algoritma kriptografi lainnya seperti watermarking dan steganografi.Watermarking berguna untuk menghindari pemalsuan,steganografi bermanfaat untuk menhindari kecurigaan.

Metode ini juga kurang dapat digunakan untuk autentikasi karena noise yang dihasilkan sangat besar.Untuk mengurangi noise tersebut maka kombinasi warna perlu diperbanyak.Sehingga dapat mengurangi warna hitam atau putih.

REFERENCES

Chang Hou,Visual Crypthography for Color Image, Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC,2002.

Lio Franklyn Kemit, Kriptografi Visual Berwarna dengan Metode Halftone,Makalah Kriptografi,Teknik Informatika,Institut Teknologi Bandung,2012.

Nazanin Askari, Cecilia Moloney, Howard M. Heys Application of Visual Cryptography to Biometric Authentication, Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, Canada.

P.S.Revenkar Anisa Anjum W .Z.Gandhare.Secure Iris Authentication Using Visual Cryptography. Department of Computer Science and Engineering. Government College of Engineering, Aurangabad, Maharashtra, India,2010.

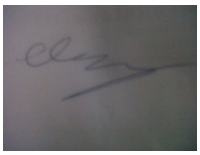
L. W. Hawkes, A. Yasinsac, C. Cline. An Application of Visual Cryptography To Financial Documents. Security and Assurance in Information Technology Laboratory, Computer Science Department, Florida State University, Tallahassee.

P.S.Revenkar, Anisa Anjum, W .Z.Gandhare.Survey of Visual Cryptography Schemes. Government College of Engineering, Aurangabad, M.S., India,2010.

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, 19 Mei 2013



Everaldo Sembiring
13510095