ISSN 2085-4552

Implementasi Skema Meaningful Sharing pada Kriptografi Visual Berwarna untuk Digital Safe Deposit Box

Willy Sudiarto Raharjo, Danny Aguswahyudi
Program Studi Teknik Informatika Fakultas Teknologi Informasi UKDW Yogyakarta, Indonesia
willysr@ti.ukdw.ac.id, danny.a@ti.ukdw.ac.id

Diterima 25 Maret 2016
Disetujui 28 Mei 2016

Abstract— **Conventional key being used in safe deposit box is a physical key that is easily duplicated, stolen and abused by irresponsible parties. This research proposed a model that substitutes the conventional key with a digital shared secret with the use of visual cryptography scheme. Visual cryptography hide the secret image into two or more images which are called share images that will not reveal anything about secret image if they were separated. The secret image can be recovered simply by stacking the shared images together without any complex computation. In this research, we propose a digital safe deposit box built using a color visual cryptography scheme. The proposed system will generate secret images containing passphrase that will be hidden in two shared images. The shared images are used for substituting the traditional key. We found 93% of the stacked image are visually readable by human eye and Arial-Courier font combination are more readable compared to Times New Roman-Calibri with 95% compared to 92% during human visual verification process.**

Index Terms— visual cryptography, secret sharing

I. Pendahuluan

Dewasa ini, menyimpan barang berharga seperti perhiasan mahal, barang-barang langka dan juga berkas-berkas penting di rumah pribadi dirasa sudah tidak aman lagi. Ancaman pencurian, kebakaran atau mungkin bencana alam menjadi sebuah pertimbangan tersendiri. Oleh karena itu, orang mulai beralih menggunakan safe deposit box untuk menyimpan barang-barang berharganya. Walaupun barang tersebut lebih terjamin, tetapi masih ada permasalah yang dihadapi oleh pengguna. Karena prosedur untuk membuka safe deposit box adalah dengan menggunakan dua buah kunci, kunci dari bank dan juga kunci yang dimiliki oleh nasabah, sehingga muncul permasalahan baru bagi nasabah yaitu menyimpan kunci untuk membuka pintu safe deposit box. Selain ada kemungkinan lupa di mana menyimpan kuncinya, kunci tersebut juga mudah untuk diduplikasi.

Salah satu cara untuk menanggulangi masalah tersebut adalah mengubah objek kunci nyata menjadi sebuah kunci digital yang lebih mudah, nyaman dan menggunakan *one-time password* agar tidak mudah diduplikasi. Keamanan pada kunci digital tersebut juga perlu ditingkatkan. Salah satu cara untuk melindungi kerahasiaan tersebut adalah menggunakan kriptografi visual. Fitur dari kriptografi visual adalah kemampuannya untuk mengembalikan gambar yang dirahasiakan tanpa menggunakan komputasi apapun. Kriptografi Visual memanfaatkan kemampuan visual manusia untuk membaca pesan rahasia dari penumpukan beberapa gambar yang digunakan untuk memunculkan kembali gambar yang dirahasiakan. Tidak ada kebutuhan komputasional yang tinggi untuk mendapatkan kembali informasi yang sudah disembunyikan. Semua proses dekripsi dilakukan oleh *human visual system* [1].

Penelitian ini menggunakan skema *meaningful sharing* kriptografi visual berwarna untuk membangun sebuah sistem digital safe deposit box.

II. TINJAUAN PUSTAKA

Penelitian tentang visual kriptografi sudah pernah dilakukan oleh beberapa peneliti. Salah satunya adalah Hsien-Chu Wu, Hao-Cheng Wang, dan Rui-Wen Yu di tahun 2008 yang menguraikan tentang sebuah skema yang memanfaatkan visual kriptografi berwarna untuk menghasilkan sebuah *meaningful shares* [2]. Langkah-langkah yang digunakan pada penelitian ini terdiri dari *halftone transformation* yaitu pengubahan gambar berwarna menjadi gambar *halftone* berwarna. Langkah kedua adalah proses *pixel extraction* yaitu proses mengekstrak pixel dari gambar *halftone* yang sudah dihasilkan sebelumnya. Selanjutnya adalah proses *encoding* yang memanfaatkan dua buah gambar *cover* yang berukuran N x N pixel untuk menyembunyikan gambar *secret* yang berukuran N x N pixel dan menghasilkan dua buah gambar *share* berukuran 2N x 2N pixel. Walaupun pada proses pengubahan gambar berwarna menjadi gambar *halftone* menghasilkan ukuran block yang terekspansi

menjadi 2N x 4N, gambar *share* yang dihasilkan tetap hanya terekspansi menjadi 2N x 2N. Hal ini dikarenakan adanya proses *pixel extraction* yang merupakan salah satu proses penting dalam penelitian ini, sehingga akan lebih menghemat penyimpanan. Selain itu penelitian ini menghasilkan gambar *share* yang tidak nampak seperti gambar dengan *random noise* dan mata manusia masih dapat mengenali gambar share tersebut dikarenakan tingkat warna kontrasnya masih lebih dari 60% serta berhasil untuk menyembunyikan gambar *secret*.

Visual kriptografi juga telah dimanfaatkan untuk melakukan proses otentikasi pengguna pada aplikasi perbankan [3]. Pada penelitian ini, obyek yang digunakan adalah tandatangan dari nasabah dan untuk pemrosesan menggunakan teknik korelasi. Selain untuk proses otentikasi pengguna, juga bisa digunakan untuk proses verifikasi server [4].

Penelitian lain dilakukan pada tahun 2007 oleh Shyong Jian Shyu, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, dan Kun Chen yang memaparkan tentang pengembangan dari skema kriptografi visual berbasis *circle shares* [5] untuk *secret* lebih dari 1 dengan menggunakan *circle share* [6].

III. LANDASAN TEORI

A. Secret Sharing

Secret sharing merupakan sebuah metode dimana rahasia didistribusikan ke beberapa partisipan dan masing-masing partisipan memiliki sebagian dari keseluruhan *secret* yang ada. Potongan-potongan *secret* tersebut disebut sebagai *share*. *Secret* hanya bisa disusun kembali ketika jumlah *share* yang ada mencukupi untuk dikombinasikan dan membuka pesan rahasia tersebut. Ketika *share* terpisah, maka tidak ada informasi mengenai *secret* yang bisa diakses. Oleh karena itu, *share* benar-benar tidak bisa dipakai apabila dalam kondisi terpisah.

Dalam skema *secret sharing*, sebuat *secret* dibagi menjadi beberapa *shares* dan didistribusikan ke n orang. Ketika k atau lebih orang ($k \leq n$) mengkombinasikan *share* masing-masing secara bersama-sama, *secret* tidak bisa direkonstruksi ulang. Jika k – 1 orang berupaya untuk merekonstruksi *secret*, tetap tidak akan berhasil. Oleh karena skema tersebut, sistem *secret sharing* seperti ini disebut skema (k, n) – threshold atau *k-out-of-n secret sharing*.

B. Error Diffusion

Sam Hocevar dan Gary Niger berargumen bahwa Error Diffusion adalah salah satu teknik halftone yang dikembangkan oleh Floyd dan Steinberg pada tahun 1976 [7] [8]. Teknik ini digunakan untuk mengkompensasi kesalahan pada proses *thresholding*. Berikut ini penjabaran mengenai metode *error diffusion* oleh Floyd-Steinberg:

$$b(i,j)\begin{cases}255 \text{ if } f(i,j) > T \\ 0 \text{ else}\end{cases} \quad (1)$$

$$e(i,j) = f'(i,j) - b(i,j) \quad (2)$$

$$f'(i,j) = f(i,j) + \sum_{k,l \in S} h(k,l)e(i-k, j-l) \quad (3)$$

Filter yang dikembangkan oleh Floyd-Steinberg dapat dilihat pada Gambar 1.

	•	7/16
3/16	5/16	1/16

Gambar 1. Error Diffusion Filter

Keterangan :

$f(i,j)$=*pixel* pada posisi (i, j) yang *diinputkan*

$f'(i,j)$=penjumlahan dari *input pixel* dan *diffused error*

$b(i,j)$=*quantized pixel value*

$h(k,l)$=*diffusion filter* yang dimana $\sum h(k,l) = 1$

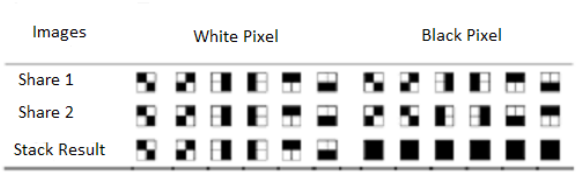
$e(i,j)$=selisih dari nilai dari *pixel* baru dengan *quantized pixel value*

C. Kriptografi Visual

Kriptografi visual diperkenalkan pertama kali oleh Naor dan Shamir pada tahun 1994 [9]. Kriptografi Visual merupakan teknik kriptografi yang memungkinkan informasi citra di-encode sedemikian rupa sehingga dalam proses decoding-nya bisa dilakukan tanpa bantuan komputasi dari komputer melainkan menggunakan sistem visual mata manusia.

Pada skema secret sharing (2,2)-threshold, digunakan citra *secret* berupa citra binary dengan dimensi N × N. Pertama, semua pixel diekspansi menjadi 2 × 2 block, dan setiap block terbentuk dari 2 buah pixel hitam dan 2 buah pixel putih seperti pada Gambar 2. Mengacu pada *coding table* pada yang telah didefinisikan pada Gambar 3, sebuah block dapat dibuat sesuai dengan pixel dari citra *secret*. Ketika semua pixel sudah selesai diproses, maka dua citra *share* sudah selesai dibuat dan dengan menumpukkan kedua *share*, kita bisa mendapatkan citra *secret* kembali. Setelah proses encoding, ukuran citra *share* menjadi 2N × 2N.

Gambar 2. Block 2x2



Gambar 3. Coding Table

Berikut ini adalah *secret image pixel coding rule:*

1. Sistem akan memilih salah satu bentuk *block* secara *random* seperti pada Gambar 2.
2. Sebuah *pixel* pada citra *secret* akan disesuaikan dengan *coding table* untuk membuat *share1* dengan bentuk *block* yang sudah dipilih sebelumnya.
3. Sistem membentuk *share2* dengan melakukan pencocokan dengan *block* pada *share1* dengan mengacu kembali pada Coding Table seperti pada Gambar 3.

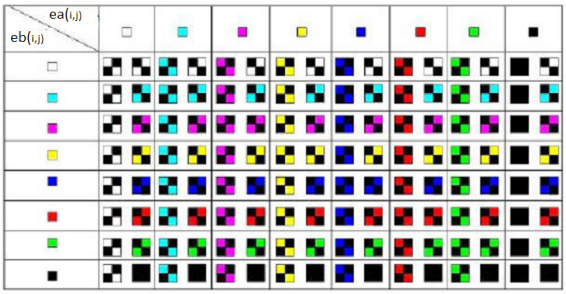
Sistem melakukan langkah 1 sampai 3 sampai semua *pixel* sudah dirubah menjadi *block.*

Algoritma kriptografi visual oleh Hsien-Chu Wu, Hao-Cheng Wang dan Rui-Wen Yu merupakan algoritma yang berdasarkan pada kriptografi visual Naor dan Shamir pada tahun 1994 [9] dan algoritma kriptografi visual dari Hou pada tahun 2003 [10]. Pada proses encoding diperlukan 3 buah citra, yaitu 2 buah citra yang digunakan untuk menyembunyikan 1 buah citra rahasia. Akan tetapi, setelah dienkripsi mata manusia tetap mampu mengenali 2 citra sampul (*share*) tersebut. Oleh karena alasan tersebut skema kriptografi visual ini disebut dengan *Meaningful Share*. Sedangkan untuk proses decoding dilakukan dengan menumpuk (*stacking*) *share* yang ada dan memanfaatkan kemampuan visual manusia.

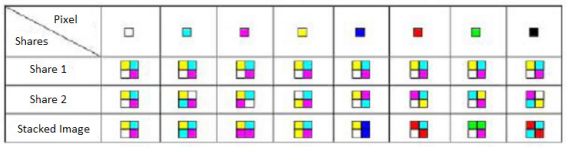
Encoding

Menurut algoritma kriptografi visual oleh Hsien-Chu Wu, Hao-Cheng Wang proses pertama pada *preprocessing* yaitu *color halftone transformation,* mengubah citra *continuous tone* menjadi citra berwarna *halftone* yang bertujuan untuk *thresholding.* Proses kedua adalah *pixel extraction*, melakukan ekstraksi *pixel* dari citra *halftone* untuk memperkecil dimensi citra. Proses utamanya adalah pembentukan citra *shares* dengan menggunakan *Code Coding Table (CCT)* dan *Secret Coding Table (SCT)*. CCT dan SCT ditunjukkan pada Gambar 4 dan Gambar 5.

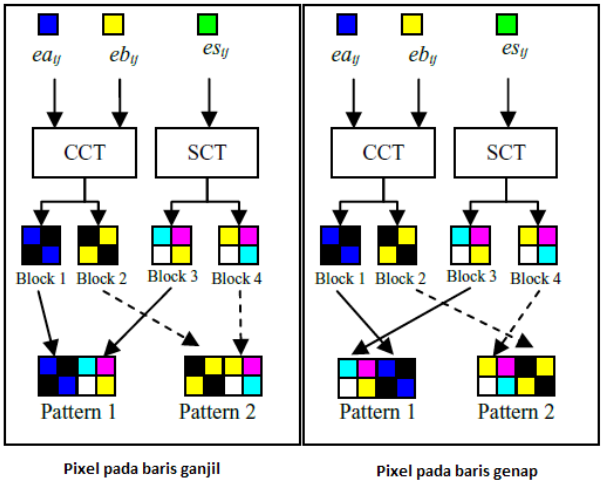
Dalam pembentukan *shares*, dua buah $N \times N$ *cover image* (CA dan CB), digunakan untuk melakukan *encoding* pada $N \times N$ *secret image* (SI) dan membentuk dua buah $2N \times 2N$ *shares* (*share1* dan *share2*) seperti pada Gambar 6.



Gambar 4. Code Coding Table



Gambar 5. Secret Coding Table



Gambar 6. Proses Pembentukan Share

Berikut ini adalah prosedur dari skema Hsien-Chu Wu yang dilakukan dalam proses *encoding:*

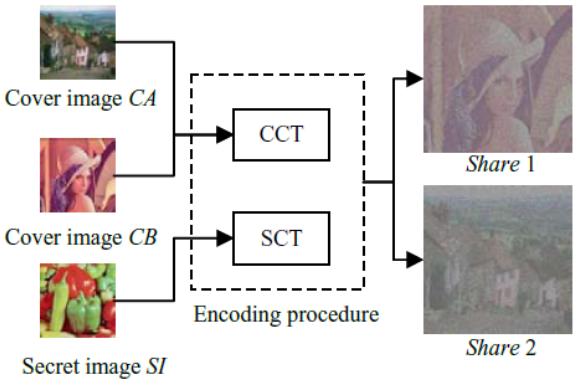
1. Dipergunakan citra *cover* (CA dan CB) berdimensi $N \times N$ untuk melakukan *encoding* pada citra *secret* (SI) berdimensi $N \times N$
2. Melakukan *preprocessing* pada citra CA, CB, SI.
   a. *Halftoning* dengan algoritma *Floyd-Steinberg* pada citra CA, CB, SI untuk *thresholding* sehingga menghasilkan citra *halftone* CA', CB', dan SI'
   b. *Pixel extraction* pada masing-masing citra CA', CB' dan SI' yaitu menghilangkan *pixel* dari citra pada kolom genap atau kolom ganjil, sehingga menghasilkan citra berukuran ½ $N \times N$ (EA, EB, dan ES).
3. Mengubah *pixel* pada citra EA dan EB menjadi *block* dengan mengacu pada CCT pada Gambar 4. Masing-masing *pixel* EA(i, j) dan EB(i, j)

disesuaikan dengan CCT, perpotongan antara warna *pixel* EA(i, j) dan EB(i, j) pada table merupakan *block* yang akan digunakan untuk pembentukan *shares*. *Block* sebelah kiri untuk citra *share1 (block1)* dan sebelah kanan untuk citra *share 2 (block2)*.

4. Mengubah *pixel* pada citra ES(i, j) menjadi dua buah *block* dengan mengacu pada SCT pada Gambar 5. *Block* untuk *share1* didefinisikan sebagai *block3* dan *block* untuk *share2* didefinisikan sebagai *block4*.
5. Membentuk citra *share1* dan *share2* seperti pada Gambar 7
   a. Jika *pixel* EA(i, j) EB(i, j) dan ES(i, j) berada pada baris ganjil maka:
      - *share1* terbentuk dari *block1* dan *block3* yang disusun berurutan
      - *share2* terbentuk dari *block2* dan *block4* yang disusun berurutan

   b. Jika *pixel* EA(i, j) EB(i, j) dan ES(i, j) berada pada baris genap maka:
      - *Share1* terbentuk dari *block3* dan *block1* yang disusun berurutan
      - *share2* terbentuk dari *block4* dan *block2* yang disusun berurutan
6. Mengulangi langkah 3 sampai 5 hingga semua *pixel* dari citra EA, EB, dan ES sudah dirubah menjadi *block.*

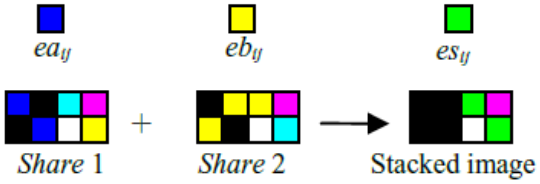
Penggabungan *block* dalam pembentukan *shares* mengakibatkan *share* yang dihasilkan berukuran 2*N* × *2N.*



Gambar 7. Prosedur encoding

Decoding

Proses *decoding* pada skema kriptografi visual Hsien-Chu Wu sama seperti dengan skema kriptografi visual pada umumnya, yaitu dengan melakukan penumpukan beberapa citra *shares* untuk menampilkan citra *secret* yang dengan mudah dapat dikenali oleh mata manusia. Proses penumpukan ini divisualisasikan pada Gambar 8.



Gambar 8. Penumpukan Gambar Share

Proses penumpukan *share* dalam bahasa pemrograman dapat dilakukan dengan menggunakan operasi AND pada nilai-nilai dari RGB masing-masing *pixel.* Contoh penumpukannya dapat dilihat pada Tabel 1 dan Tabel 2.

Tabel 1 Informasi Share 1 dan 2

Pixel(i, j) pada *share 1*				*Pixel(i, j)* pada *share 2*			
Warna	Red	Green	Blue	Warna	Red	Green	Blue
Y	255	255	0	M	255	0	255
C	0	255	255	Y	255	255	0
M	255	0	255	C	0	255	255

Tabel 2 Hasil operasi AND

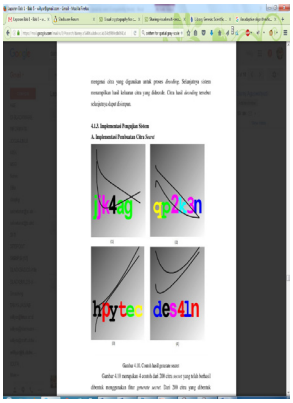
Hasil operasi AND pada *Pixel(i, j)*			
Warna	Red	Green	Blue
R	255	0	0
G	0	255	0
B	0	0	255

IV. IMPLEMENTASI SISTEM

Pertama-tama ditentukan dahulu citra yang akan digunakan sebagai gambar rahasia (*secret*). Untuk membantu dalam proses pengujian, pesan rahasia (*passphrase*) dituliskan kedalam sebuah citra seperti layaknya sistem CAPTCHA yang dihasilkan secara random dengan ukuran 300x300 pixel dan menggunakan 2 jenis kombinasi font yang berbeda, yaitu Arial-Courier dan Times New Roman-Calibri. Citra tersebut akan mengalami pre-processing terlebih dahulu yaitu dengan *half-toning* dan *pixel-extraction*. Contoh gambar rahasia ditunjukkan pada Gambar 9.

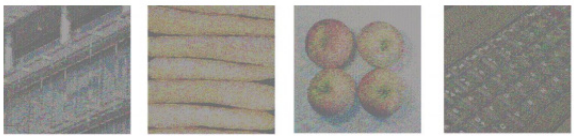
Citra tersebut kemudian masuk ke proses encoding seperti pada Gambar 7 dan di-encode dengan menggunakan dua citra *cover* yang berbeda (Gambar 10). Hasil keluaran dari proses ini adalah dua buah gambar *share* baru (Gambar 11 dan Gambar 12) yang digunakan untuk merekonstruksi ulang gambar rahasia.

Pada proses rekonstruksi ulang, kedua gambar *share* ditumpuk (*stack*) dan akan menghasilkan sebuah gambar baru yang menunjukkan pesan rahasia yang terkandung didalam gambar rahasia (Gambar 13).

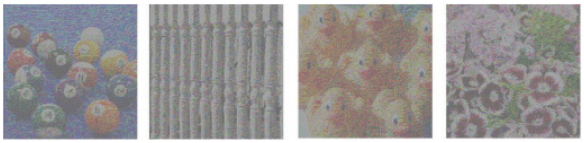


Gambar 9. Contoh Gambar Rahasia

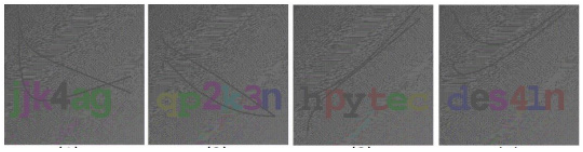
Gambar 10. Contoh Gambar Cover



Gambar 11. Hasil Share1



Gambar 12. Hasil Share2



Gambar 13. Hasil Decoding

V. PENGUJIAN SISTEM

Untuk pengujian apakah mata manusia masih mampu mengenali citra *secret* serta membaca pesan yang ditambahkan pada citra, maka akan dilakukan pengujian langsung terhadap 20 responden yang berkisar antara 18-33 tahun dimana semuanya tidak memiliki masalah buta warna partial atau penuh, tetapi masih dimungkinkan memiliki kesehatan mata yang berbeda-beda. Setiap responden akan mendapatkan 20 hasil pembentukan kembali dari citra *secret* dan diminta untuk menuliskan kembali *passphrase* yang tertera pada citra. Proses selanjutnya adalah membandingkan hasil yang diberikan oleh responden dengan *passphrase* yang dihasilkan oleh sistem saat *generating* citra *secret.*

Penggunaan font yang berbeda memungkinkan terjadinya perbedaan dalam pendeteksian *passphrase*. Untuk membuktikannya, masing-masing font akan diujikan ke 10 responden. **Tabel 3** dan **Tabel 4** menggambarkan persentase gambar yang terbaca dengan benar dengan menggunakan font Arial-Courier dan Times New Roman-Calibri. Pemilihan dua responden yang berbeda ini untuk menghindari nilai bias yang disebabkan karena kondisi mata yang sudah terbiasa dengan satu jenis font tertentu.

Tabel 3 Persentase keberhasilan deteksi dengan font Arial-Courier

Responden	Jumlah Citra Uji	Jumlah Hasil Respon Benar	Persentase Terbaca
Responden 1	20	16	80%
Responden 2	20	20	100%
Responden 3	20	20	100%
Responden 4	20	18	90%
Responden 5	20	19	95%
Responden 6	20	20	100%
Responden 7	20	20	100%
Responden 8	20	16	80%
Responden 9	20	20	100%
Responden 10	20	20	100%
Total	**200**	**189**	**95%**

Tabel 4 Persentase keberhasilan deteksi dengan font Times New Roman-Calibri

Responden	Jumlah Citra Uji	Jumlah Hasil Respon Benar	Persentase Terbaca
Responden 11	20	18	90%
Responden 12	20	19	95%
Responden 13	20	19	95%
Responden 14	20	17	85%
Responden 15	20	19	95%
Responden 16	20	20	100%
Responden 17	20	17	85%
Responden 18	20	18	90%
Responden 19	20	18	90%
Responden 20	20	18	90%
Total	**200**	**183**	**92%**

Berikut ini adalah penjelasan mengenai tabel di atas:

- Responden adalah responden keberapa yang melakukan pengujian.
- Jumlah citra uji merupakan jumlah citra hasil *decoding* yang digunakan untuk pengujian yang dimana pada setiap citra terdapat *passphrase* yang berbeda.
- Jumlah hasil respon benar adalah merupakan jumlah *passphrase* yang ditulis kembali oleh responden secara benar.
- Persentase terbaca merupakan persentase dari perbandingan jumlah citra yang diuji dan hasil respon yang benar.

Berdasarkan hasil pengujian dengan responden dapat diketahui bahwa tingkat akurasi sistem dalam memunculkan kembali citra *secret* cukup tinggi yaitu mencapai 93%. Hal ini ditunjukkan dengan tingginya kemampuan para responden dalam menuliskan kembali *passphrase* yang ada pada citra hasil *decoding*.

Karena responden masih mampu mengenali citra hasil *decoding* dan hasil pembentukan *share* maka sistem dapat dikatakan berhasil melakukan pembentukan *meaningful share,* walaupun ketajaman citra yang dihasilkan cukup berkurang dan cenderung lebih gelap. Kekurangan tersebut dikarenakan pada saat pembentukan citra *share* banyak menggunakan *pixel* hitam dalam pembentukan *block* sehingga hasil citra cenderung lebih gelap.

Setelah mencermati kembali hasil respon dari responden, dapat dilihat bahwa pembentukan *passphrase* menggunakan *font Arial-Courier* memiliki persentase keberhasilan 95%. Sedangkan pembentukan *passphrase* menggunakan *font Times New Roman-Calibri* memiliki persentase keberhasilan 92%. Berdasarkan hasil tersebut, maka dapat diketahui bahwa mata manusia lebih mudah mengenali *passphrase* yang dibentuk dengan *font Arial-Courier.*

VI. IMPLEMENTASI NYATA

Sistem yang dibangun masih berupa prototype dan berfokus pada mekanisme pembuatan serta penggabungan file *share* untuk merekonstruksi kunci digital. Untuk bisa direalisasikan menjadi sebuah produk yang benar-benar bisa digunakan, maka perlu mempertimbangkan banyak aspek, misalnya regulasi pemerintah atau kebijakan internal perusahaan, mekanisme dan standarisasi dalam hal pendistribusian informasi ke N pihak serta mekanisme keamanan lainnya yang perlu diperhatikan.

VII. KESIMPULAN

Berdasarkan pembahasan dan analisis terhadap hasil pengujian sistem pada bab 4, maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Metode kriptografi visual berwarna oleh Hsien-Chu Wu, Hao-Cheng Wang dan Rui-Web Yu dapat digunakan untuk mengimplementasi sistem digital safe deposit box. Citra share yang dihasilkan dari metode ini sama sekali tidak memberikan informasi apapun mengenai citra secret yang disembunyikan.
2. Pengimplementasian metode kriptografi visual berwarna oleh Hsien-Chu Wu, Hao-Cheng Wang dan Rui-Web Yu berhasil menghasilkan citra *share* dan citra *secret* yang *meaningful*, sehingga citra yang dibentuk tidak menghasilkan citra berupa abstrak.
3. Citra yang dihasilkan cenderung lebih gelap dari citra awal dan ketajamannya berkurang.
4. Pemanfaatan kombinasi font Arial dan Courier menghasilkan persentase keberhasilan yang tinggi yaitu 95% dibandingkan dengan kombinasi Times New Roman dan Calibri yang menghasilkan nilai 92%, namun beberapa huruf kecil dan angka yang bentuknya mirip berpotensi meningkatkan tingkat ambiguitas dan mengurangi persentase keberhasilan pendeteksian oleh mata manusia.

VIII. SARAN

Beberapa saran yang dapat menjadi masukan untuk penelitian selanjutnya:

1. Menggunakan jumlah warna palette untuk *thresholding* lebih dari 8 warna sehingga dapat menambah ketajaman warna.
2. Memilih font yang dapat menghindari ambiguitas angka dengan huruf serta menggunakan *uppercase* dan *lowercase* untuk memperbanyak variasi *passphrase* yang dibentuk. Misalkan saja mengganti font menjadi Calibri dan menghilangkan angka 0.
3. Ukuran font harus disesuaikan dengan panjang text *passphrase* dan ukuran citra agar tidak terjadi kemungkinan kesalahan saat *generating secret* seperti angka atau huruf yang terpotong saat ditambahkan pada citra.

Daftar Pustaka

[1] Weir, Jonathan, Yan, WeiQi, "A Comprehensive Study of Visual Cryptography", Transactions of DHMS LNCS 6010, Springer, hal 70-105, 2010.

[2] Wu, Hsien-Chu, Hao-Cheng Wang, and Rui-Wen Yu. "Color visual cryptography scheme using meaningful shares." *Intelligent Systems Design and Applications, 2008. ISDA'08. Eighth International Conference on*. Vol. 3. IEEE, 2008.

[3] C. Hedge, M. S., D. Shenoy, V. KR., M. Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications", *Advanced Computing and Communications, 2008. ADCOM 2008. 16th International Conference on*. IEEE, 2008.

[4] A. Bhanji, P. Jadhav, S. Bhujbal, P. Mulak, "Secure Server Verification By Using RSA Algorithm And Visual Cryptography", International Journal of Engineering Research & Technology, Vol.2 - Issue 4 (April), 2013.

[5] W. Hsien-Chu, C. Chin-Chen, "Sharing visual multi-secrets using circle shares", Computer Standards & Interfaces Vol 28, Issue 1, 2005, hal. 123–135.

[6] S. Shyong Jian, H. Shih-Yu, L. Yeuan-Kuen, W. Ran-Zan, C. Kun, "Sharing multiple secrets in visual cryptography", *Pattern Recognition*, vol *40 issue* 12, 2007, hal 3633-3651.

[7] R. W. Floyd, L. Steinberg. "An adaptive algorithm for spatial grey scale", Proceedings of the Society for Information Display, Vol 17, Number 2, 1976, hal 75-77.

[8] S. Hocevar, G. Niger. "Reinstating floyd-steinberg: Improved metrics for quality assessment of error diffusion algorithms." Image and Signal Processing. Springer Berlin Heidelberg, 2008, hal 38-45.

[9] M. Naor, A. Shamir, "Visual Cryptography". Advances in Cryptology-EUROCRYPT"94, 1995, hal 1-12,

[10] H. Young-Chang, "Visual Cryptography for Color Images", Pattern Recognition, Vol 36, Issue 7, 2003, Hal 1619-1629.