Perbandingan Metode Enveloping BPCS dan DE dalam Kriptografi Visual dengan Tambahan Noise

Ronsen Purba[1], Ali Akbar Lubis[2], Wulan Sri Lestari[3]
Prodi Teknik Informatika
STMIK Mikroskil
Medan, Indonesia
Email: ronsen@mikroskil.ac.id, ali.akbar@mikroskil.ac.id, wulanlestari32@gmail.com

Abstrak—Skema (k, n) *secret sharing* menghasilkan n *shares* menggunakan angka acak sehingga citra dapat direkonstruksi dengan *k* buah *shares* (2≤*k*≤n). Namun, teknik ini memungkinkan setiap orang yang memiliki *k* buah *shares* dapat melakukan proses rekonstruksi. Untuk menghilangkan kecurigaan pihak ketiga terhadap hasil enkripsi citra masukan dapat diatasi dengan teknik pengamplopan. Dalam penelitian ini diterapkan dua jenis metode pengamplopan yakni *Digital Enveloping* (DE) dan *Bit Plane Complexity Segmentation* (BPCS). Kedua metode dibandingkan dalam hal waktu sisip dan ekstraksi, *fidelity*, dan tingkat pengembalian citra jika amplop yang berisi *share* diberikan *noise* (*robustness*). Hasil pengujian menunjukkan bahwa waktu sisip dan ekstrak DE jauh mengungungguli BPCS. Tetapi dari sisi *fidelity*, metode BPCS sedikit lebih baik dibandingkan dengan DE. Sedangkan untuk *recovery rate* dengan distribusi *uniform*, DE lebih baik dibandingkan BPCS serta untuk distribusi *salt&pepper* kedua metode memberikan hasil yang hampir sama.

Kata Kunci— ***Kriptografi Visual; DE; BPCS Fidelity; Robustness***

I. PENDAHULUAN

Kriptografi visual adalah teknik pengamanan citra dimana proses enkripsi dilakukan dengan membagi citra asli menjadi beberapa *shares* sehingga dapat didekripsi oleh sistem visual manusia [1]. Skema *(k,n) secret sharing* membentuk *n* buah *shares* menggunakan angka acak sehingga dapat direkonstruksi dengan menyusun minimal *k* shares. Kelemahan skema ini yaitu proses rekonstruksi citra dapat dilakukan oleh siapa saja yang memiliki minimal *k shares* [2]. Bhakta et al, 2013 mengatasi kelemahan tersebut dengan menerapkan *image key* pada skema (*k,n*) *secret sharing*. *Image key* digunakan untuk mengenkripsi citra asli sebelum dibagi menjadi n shares [3]. Namun, cara ini juga memiliki kekurangan yaitu citra hasil enkripsi (*cipher image*) masih memperlihatkan pola citra aslinya. Untuk menghilangkan pola citra asli pada *cipher image*, maka dapat digunakan teknik pengamanan citra lainnya yaitu pengacakan, misalnya menggunakan *Non-linear Chaotic Algorithm* (NCA). Hasil analisis oleh Gao et al, enkripsi citra menggunakan NCA menunjukkan *cipher image* tidak dapat dikenali, piksel-pikselnya tidak saling berhubungan, ruang kunci yang besar dan keamanan yang tinggi [4]. Kemudian cipher image dibagi menjadi n buah *shares*. Namun, teknik ini dapat menimbulkan kecurigaan pihak lain.

Untuk menghilangkan kecurigaan tersebut, maka digunakan metode pengamplopan (*enveloping*). Tujuannya adalah untuk menyembunyikan shares ke dalam gambar sebagai sampul, sehingga dapat meningkatkan keamanan pesan. Ada beberapa teknik yang umum digunakan untuk tujuan tersebut seperti *least significant bit* (LSB), *sampling error* dalam *image digitization*, dan teknik frekuensi spasial. Eiji Kawaguchi dan Richard O. Eason memperkenalkan sebuah metode penyembunyian pesan yang disebut dengan *Bit Plane Complexity Segmentation* (BPCS). Metode ini tidak berdasarkan pada teknik pemrograman tetapi memanfaatkan karakteristik penglihatan manusia yang tidak mampu menginterpretasikan pola biner yang sangat rumit. Kelebihan BPCS adalah memiliki kapasitas penyimpanan pesan yang relatif besar [5]. Kapasitas pesan yang disisipkan dapat mencapai 50% dari ukuran citra amplop [6]. Selain BPCS, dapat digunakan metode *Digital Enveloping* (DE) yang merupakan metode pengamplopan sederhana serta menyediakan kapasitas penyimpanan pesan yang cukup besar dan memiliki cara kerja yang sama seperti LSB [7]. Pada tahun 2013, Das et al melakukan pengujian menggunakan DE pada citra amplop dan *share* untuk mengetahui perubahan warna pada citra amplop. Hasil pengujian mereka menunjukkan jika dua bit terakhir dari masing-masing piksel citra amplop diubah dengan bit piksel share, maka perubahan warna pada citra amplop tidak dapat dibedakan oleh sistem visual manusia [7].

Dalam penelitian ini dibangun sebuah aplikasi untuk pengamanan citra warna dengan menerapkan kriptografi citra NCA dan kriptografi visual dengan teknik pengamplopan DE dan BPCS. Tujuan penelitian adalah membandingkan kinerja metode pengamplopan DE dan BPCS, dalam hal: (1) waktu penyisipan dan ekstraksi, (2) kapasitas muatan (*fidelity*) menggunakan nilai PSNR, dan (3) ketangguhan (*robustness*) yakni tingkat pengembalian citra asli apabila satu atau sebagian amplop yang berisi *share* diberi *noise*.

II. TINJAUAN PUSTAKA

A. Metode *NonLinear Chaotic Algorithm* (NCA)

NonLinear Chaotic Algorithm merupakan algoritma pembangkit bilangan acak (PRNG) yang dikembangkan oleh Haojiang Gao, Yisheng Zhang, Shuyun Liang dan Dequn Li dalam dengan judul “A new chaotic algorithm for image

encryption“. Persamaan NCA memanfaatkan fungsi tangen dan fungsi perpangkatan, sebagai berikut [4]:

$$x_{i+1} = \lambda * \tan(\alpha x_i) * (1 - x_i)^{\beta}$$

dimana ∈(0,1), i = 1,2,3,4…. n dan > jika = 1/(1+β). Sedangkan untuk parameter λ akan dijelaskan pada persamaan berikut:

$$\lambda = \mu * ctg\left(\frac{\alpha}{1+\beta}\right) * \left(1+\frac{1}{\beta}\right)^{\beta}$$

μ = 1 – β-4 > 0. Jadi persamaan NCA didefinisikan sebagai berikut:

$$x_{i+1} = [1-\beta^{-4}] * ctg\left(\frac{\alpha}{1+\beta}\right) * \left(1+\frac{1}{\beta}\right)^{\beta} * \tan(\alpha * x_i) * (1-x_i)^{\beta}$$

dimana ∈ (0, 1), α ∈ (0,1.4], β ∈ [5,43], atau ∈ (0, 1), α ∈ (1.4,1.5], β ∈ [9,38], atau ∈ (0, 1), α ∈ (1.5,1.57], β ∈ [3,15].

Proses enkripsi terdiri dari RGB *shuffle* yang digunakan untuk mengacak susunan RGB serta *encoding* yang digunakan untuk mengubah nilai RGB. RGB *shuffle* dan *encoding* memanfaatkan konsep multithreading, yang dibagi ke dalam 3 *threads*. Penjelasan masing-masing *thread* dapat dilihat berikut ini:

1. Thread 1

   Thread ini digunakan untuk membangkitkan deretan bilangan acak sebanyak $M \times N \times 3$, dimana *M* merupakan panjang citra dan *N* merupakan lebar citra, kemudian deretan bilangan acak diduplikasi ke variabel *t* dan diurutkan secara menurun. Selanjutnya bilangan acak tersebut dikonversi dari bilangan real ke bilangan bulat menggunakan persamaan:

$$T(x, size) = \| x * 10^{count} \|, x \neq 0$$

   dimana count dimulai dari 1 dan bertambah 1 sampai $x*10^{count} > 10^{size-1}$. Hasilnya kemudian diambil bagian bulatnya saja. Sebagai contoh, misalkan x = 0.0005467854 dan size = 4, maka dimulai dari count = 1 sampai count = 7 diperoleh 0.0005467854*107 = 5467.854 > 10^3. Kemudian ambil bagian integer ||5467.854||=5467, kemudian nilai tersebut selanjutnya dimodulokan dengan 256 dan ditampung ke dalam array K.

2. Thread 2

   Thread ini digunakan untuk mengambil nilai RGB pada citra input dan nilainya ditampung dalam array C.

3. Thread 3

   Thread ini digunakan untuk membandingkan nilai deretan acak sebelum dan sesudah diurutkan yang dibangkitkan pada *thread* 1, kemudian mengacak nilai RGB yang diambil pada *thread* 2 sesuai dengan indeks perbandingan dan ditampung dalam array C1.

Selanjutnya masuk tahap *encoding* dengan operasi :

$$C2_i = (C1_i \oplus C2_{i-1}) \oplus K_i$$

dimana :

$C2_i$ = array hasil *encoding* pada indeks ke-i
$C1_i$ = array hasil RGB *shuffle* pada indeks ke-i
K_i = array hasil konversi pembentukan kunci pada indeks ke-i

Pada proses *encoding* nilai $C2_{i-1}$ yang pertama kali adalah initialization vector (IV). Initialization vector (IV) tidak perlu rahasia tetapi harus sama nilainya pada proses dekripsi. Setelah selesai nilai-nilai yang dihasilkan dari C2 dimasukan kembali ke dalam matriks citra, sehingga dihasilkan cipher image.

Proses dekripsi adalah kebalikan dari enkripsi dimana yang dilakukan adalah *decoding* dan RGB deshuffle yang juga dibagi ke dalam 3 *thread*, hanya saja perbedaanya terletak pada *thread* 3. Proses *decoding* dilakukan dengan meng-XOR-kan nilai-nilai RGB-nyadengan kunci:

$$P1_i = (P_i \oplus K_i) \oplus P_{i-1}$$

dimana :

$P1_i$= array hasil *decoding* pada indeks ke-i
P_i = array piksel *cipher image* pada indeks ke-i

Nilai P_{i-1} yang pertama kali adalah *initialization vector* (IV). Sedangkan proses *RGB deshuffle* sama seperti proses *RGB shuffle.* Perbedaannya hanya terletak pada proses perbandingan nilai acak yang sudah diurutkan dengan nilai acak yang belum diurutkan.

B. *Kriptografi Visual*

Kriptografi visual terdiri dari 2 proses utama yaitu:

1. Proses pembentukan shares dengan langkah-langkah sebagai berikut [2]:
   a. Masukkan citra asli
   b. Hitung lebar (*w*) dan panjang (*h*) pada citra asli.
   c. Masukkan jumlah citra *share* (*n*) dan jumlah minimal citra *share* (*k*) yang dibutuhkan untuk rekonstruksi.
   d. Hitung RECONS = (*n*-*k*) + 1.
   e. Bentuk *array* tiga dimensi [n][w*h][32] untuk menyimpan setiap piksel dari jumlah citra *share* (*n*).
   f. *Scan* setiap piksel dari citra asli kemudian di konversi ke 32 bit biner.
   g. Lakukan expansi bit 1 pada setiap piksel citra asli secara acak untuk membentuk jumlah citra *share* (*n*).
   h. Bentuk *array* satu dimensi [n] untuk menyimpan setiap piksel dari citra *share* yang telah dilakukan expansi
2. Proses rekonstruksi shares dengan langkah-langkah sebagai berikut [2]:
   a. Masukkan jumlah minimal citra *share* (*k*) yang dibutuhkan untuk rekonstruksi.
   b. Hitung panjang (*h*) dan lebar (*w*) pada masing-masing citra *share* tersebut.
   c. Bentuk *array* dua dimensi [k][w*h] untuk menyimpan setiap piksel dari masing-masing citra *share*.

d. Lakukan operasi OR pada semua citra *share* yang di-*input.*

Simpan hasil operasi OR ke *array* [w*h] untuk menghasilkan citra asli.

C. Metode Digital Enveloping (DE)

Pada proses enveloping digunakan algoritma *Least Significant Bit* (LSB) dimana untuk memetakan satu piksel dari citra asli diperlukan empat piksel citra *envelope* sehingga dibutuhkan citra *envelope* dengan ukuran empat kali lebih besar daripada citra asli.

Proses kerja metode DE dibagi menjadi 2 sub proses, yakni [8]:

1. Proses Penyisipan Share dengan langkah-langkah sebagai berikut:
   a) Masukkan citra asli dan citra *envelope* kosong.
   b) Hitung lebar (*w*) dan panjang (*h*) citra asli.
   c) Hitung lebar (*w1*) dan panjang (*h1*) citra *envelope* kosong.
   d) Konversi citra *envelope* kosong ke dalam blok sebanyak $w*h$.
   e) *Scan* satu piksel dari citra asli lalu konversi ke 32 bit.
   f) Ganti dua bit terakhir dari masing-masing piksel citra *envelope* kosong dengan bit-bit piksel citra asli.
   g) Bentuk citra *envelope* berisi bit-bit citra asli.
2. Proses Ekstraksi Share dengan langkah-langkah sebagai berikut [8]:
   a) Masukkan citra *envelope* berisi bit-bit citra asli.
   b) Konversi citra *envelope* tersebut ke dalam blok sebanyak $w1*h1/4$.
   c) Ambil dua bit terakhir dari masing-masing piksel citra *envelope* tersebut untuk membentuk citra asli.
   d) Bentuk citra asli.

D. Metode Bit-Plane Complexity Segmentation (BPCS)

Bit-plane complexity segmentation (BPCS) merupakan teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998. Teknik ini merupakan teknik steganografi yang memiliki kapasitas besar, karena dapat menampung data rahasia dengan kapasitas yang relatif besar jika dibandingkan dengan metode LSB. Metode BPCS adalah teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia, yakni ketidakmampuan manusia menginterpretasi pola biner yang sangat rumit [5].

Metode BPCS terdiri dari dua sub proses, yakni penyisipan dan ekstraksi.

Proses Penyisipan Share ditempuh dengan langkah-langkah sebagai berikut [5]:

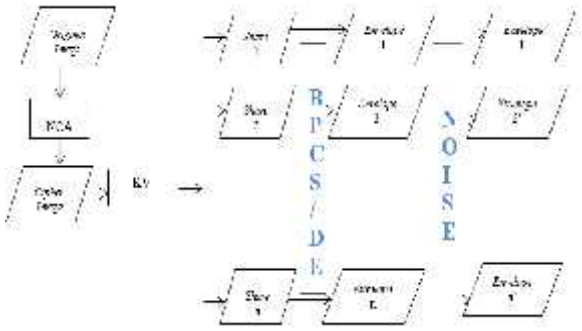
a. *Cover image* dengan sistem *PBC* diubah menjadi sistem *CGC*, kemudian gambar tersebut di-*slice* menjadi *bit-plane* dalam bentuk gambar biner. Setiap *bit-plane* mewakili bit dari setiap piksel pada gambar.
b. Segmentasi setiap *bit-plane* pada *cover image* menjadi *informative* dan *noise like region* dengan menggunakan nilai batas / *threshold* (α_0). Nilai umum dari $\alpha_0 = 0{,}3$.
c. Kelompokkan pesan rahasia menjadi rangkaian blok rahasia.
d. Jika blok (*S*) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap *S* untuk mendapatkan (*S**) yang lebih kompleks..
e. Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan *noise-like region* (atau gantikan semua bit pada *noise-like region*). Jika blok *S* dikonjugasi, maka simpan data pada "*conjugation map*".
f. Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
g. Ubah *stego-image* dari sistem *CGC* menjadi sistem *PBC*.

Proses Ekstraksi Share dengan langkah-langkah yang merupakan kebalikan dari proses penyisipan.

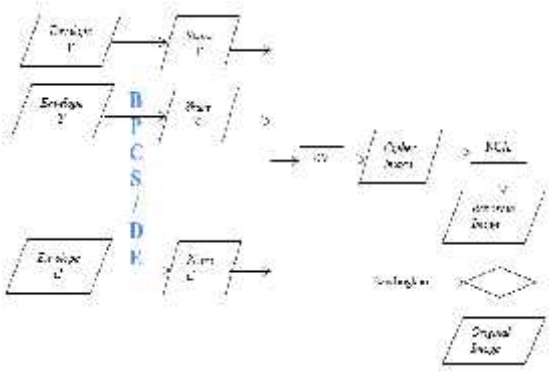
III. METODOLOGI PENELITIAN

Langkah – langkah pelaksanaan penelitian dijelaskan sebagai berikut:

1. Melakukan kajian pustaka terkait dengan metode NCA, Kriptografi Visual, DE dan BPCS.
2. Memahami proses kerja dari metode NCA, Kriptografi Visual, DE dan BPCS.
3. Analisis kebutuhan, untuk menggambarkan skema kerja penelitian seperti terlihat pada Gambar 1 dan Gambar 2 berikut ini.



Gambar 1. Proses penyisipan



Gambar 2. Proses ekstraksi

4. Merancang antar muka dan basis data
5. Membuat program
6. Melakukan pengujian terhadap kedua metode
7. Menarik kesimpulan

IV. HASIL DAN PEMBAHASAN

A. Hasil

Tampilan awal program berisi 3 pilihan, yakni: Embedding, Ekstraksi dan Pengujian seperti terlihat pada Gambar 3 berikut ini.

Gambar 3. Tampilan awal program

Apabila dipilih pengujian, maka tampilannya seperti Gambar 4 berikut ini

Gambar 4. Tampilan pengujian

Pengujian waktu kedua metode pengamplopan menggunakan 2 jenis komputer dengan tampilan seperti Gambar 5 dan Gambar 6 berikut ini.

Gambar 5. Tampilan pengujian waktu penyisipan

Gambar 6. Tampilan pengujian waktu ekstraksi

B. Hasil pengujian waktu Penyisipan dan Ekstraksi

Pengujian ini dilakukan untuk mengetahui waktu yang dibutuhkan DE dan BPCS dalam proses penyisipan dan ektraksi *share*. Untuk pengujian waktu digunakan 2 spesifikasi komputer berbeda yakni: laptop RAM: 2GB dan CPU Intel Core i3-5010U, 2.10GHz (komputer 1) dan laptop RAM : 2GB dan CPU Intel Core i3-2330M, 2.20GHz (komputer 2) dengan ukuran citra 64 x 64, 96 x 96, dan 128 x 128 dengan jumlah share = 4 sampai 10 untuk proses penyisipan. Hasil pengujian dapat dilihat pada tabel I sampai dan tabel IV di bawah ini.

TABLE I. PENGUJIAN WAKTU PENYISIPAN

No	Ukuran Citra	Jumlah Share (n)	Waktu Sisip			
			Komputer 1		Komputer 2	
			DE	BPCS	DE	BPCS
1	64 x 64	4	1.156	6.125	1.25	6.453
2		5	1.371	7.219	1.563	7.969
3		6	1.625	8.719	1.859	9.547
4		7	1.891	10.328	2.172	11.126
5		8	2.172	11.484	2.484	12.688
6		9	2.422	12.938	2.781	14.233
7		10	2.697	14.547	3.094	15.985
Rata - rata			1.904	10.194	2.172	11.146
Simpangan Baku			0.558	3.018	0.663	3.418
8	96 x 96	4	2.187	13.531	2.422	14.282
9		5	2.766	16.672	3.141	17.72
10		6	3.453	20.031	3.688	21.157
11		7	3.844	22.938	4.235	24.439
12		8	4.375	26.235	4.875	28.017
13		9	4.875	29.301	5.438	31.33
14		10	5.422	32.719	6.016	34.732
Rata rata			3.816	23.074	4.239	24.528
Simpangan Baku			1.117	6.883	1.279	7.367
15	128 x 128	4	3.1	22.906	3.922	24.782
16		5	4.484	28.766	4.985	30.736
17		6	5.359	34.329	5.922	36.767
18		7	6.281	40.391	6.985	43.018
19		8	7.172	45.798	7.86	49.139
20		9	8.219	51.829	8.969	55.581
21		10	8.969	59.355	9.969	61.909
Rata rata			6.296	40.192	6.915	43.136
Simpangan Baku			1.983	12.892	2.164	13.384

Dari Tabel I dapat dilihat bahwa semakin besar ukuran citra dan semakin banyak jumlah *share* mengakibatkan waktu sisip yang semakin lama. Kemudian tabel tersebut diperoleh waktu sisip rata-rata gabungan komputer 1 dan 2 adalah 4.235 detik dan 26.27 detik untuk metode DE dan metode BPCS secara berturut-turut. Sementara simpangan baku gabungan diperoleh 1.398 detik untuk DE dan 7.832 detik untuk metode BPCS. Dari hasil rata-rata gabungan diperoleh bahwa rasio waktu sisip antara metode DE dengan metode BPCS adalah 1 : 6.202. Sementara untuk simpangan baku gabungan diperoleh bahwa rasio antara metode DE dengan BPCS adalah 1 : 5.6.

Berdasarkan Tabel I di atas dibentuk Tabel II untuk melihat perubahan waktu sisip maksimum dan minimum akibat penambahan 1 buah *share*, masing-masing untuk komputer 1 dan komputer 2 sebagai berikut:

TABLE II. PERUBAHAN WAKTU EKSTRAK UNTUK PENAMBAHAN *SHARE*

Ukuran Citra	Perubahan Waktu untuk Penambahan 1 share		Komputer 1		Komputer 2	
			DE	BPCS	DE	BPCS
64x 64	Waktu (detik)	Maksimum	0.281	1.619	0.413	1.758
		Minimum	0.219	1.048	0.296	1.576
96x96		Maksimum	0.687	3.359	0.719	3.578
		Minimum	0.391	2.007	0.547	3.282
128x128		Maksimum	1.047	7.526	1.109	6.422
		Minimum	0.750	5.407	0.875	5.954

Dari Tabel II diperoleh bahwa semakin besar ukuran citra dan dengan penambahan 1 share mengakibatkan perubahan waktu semakin besar baik minimum maupun maksimum untuk komputer 1 dan komputer 2. Metode BPCS mengalami perubahan waktu yang lebih besar dibandingkan dengan metode DE.

Untuk mengetahui waktu ekstraksi dari kedua metode maka dilakukan pengujian pada Tabel III di bawah ini.

TABLE III. PENGUJIAN WAKTU EKSTRASI

No	Ukuran Citra	Jumlah Share (n)	Waktu Ekstraksi			
			Komputer 1		Komputer 2	
			DE	BPCS	DE	BPCS
1	64 x 64	5	0.313	1.75	0.344	1.844
2		6	0.469	2.641	0.5	2.797
3		7	0.625	3.547	0.641	3.641
4		8	0.75	4.266	0.797	4.5
5		9	0.891	5.109	0.953	5.312
6		7	1.031	5.984	1.109	6.235
7		8	1.172	6.797	1.25	7.172
8		9	1.343	7.594	1.359	7.953
9		10	1.438	8.406	1.547	8.891
Rata-rata			0.889	5.129	0.993	5.882
Simpangan Baku			0.384	2.28	0.44	2.599
10	96 x 96	5	0.75	3.891	0.766	4.172
11		6	1.047	5.781	1.203	6.266
12		7	1.422	7.719	1.516	8.766
13		8	1.781	9.672	1.891	10.484
14		9	2.078	11.531	2.234	12.453
15		7	2.359	13.266	2.531	14.344
16		8	2.75	15.172	2.953	17.111
17		9	3.094	17.063	3.32	18.491
18		10	3.344	18.813	3.578	20.193
Rata-rata			2.067	11.434	2.302	12.511
Simpangan Baku			0.898	5.114	0.962	5.591
19	128 x 128	5	1.172	6.609	1.391	7.188
20		6	1.813	10.016	1.938	10.735
21		7	2.359	13.281	2.594	14.282
22		8	2.891	16.5	3.094	17.813
23		9	3.531	19.672	3.734	21.235
24		7	4.109	23.203	4.313	24.798
25		8	4.531	26.313	4.687	28.944
26		9	5.234	29.516	5.563	32.317
27		10	5.922	32.86	6.313	35.592
Rata-rata			3.907	19.788	4.04	21.447
Simpangan Baku			1.914	9.962	1.93	10.811

Dari Tabel III di atas dapat dilihat bahwa ukuran citra dan jumlah *share* yang digunakan dalam proses ekstrak akan menambah waktu ekstraksi. Kemudian dari kedua tabel tersebut diperoleh waktu ekstrak rata-rata gabungan dengan komputer 1 dan 2 untuk metode DE adalah 2.225 detik dan 12.611 detik untuk metode BPCS. Sementara simpangan baku gabungan diperoleh 0.996 detik untuk metode DE dan 5,693 detik untuk metode BPCS. Dari hasil rata-rata gabungan diperoleh rasio waktu ekstrak antara metode DE dengan metode BPCS adalah 1 : 5.667. Sementara untuk simpangan baku gabungan diperoleh rasio antara metode DE dengan BPCS adalah 1 : 5.741.

Kemudian dari Tabel III diperoleh Tabel IV berikut ini untuk melihat perubahan waktu akibat penambahan 1 buah *share*.

TABLE IV. PERUBAHAN WAKTU EKSTRAKSI UNTUK PENAMBAHAN *SHARE*

Ukuran Citra	Perubahan Waktu untuk Penambahan 1 share		Komputer 1		Komputer 2	
			DE	BPCS	DE	BPCS
64x-64	Waktu (detik)	Maksimum	0.156	0.906	0.172	0.953
		Minimum	0.125	0.719	0.140	0.813
96x96		Maksimum	0.391	1.953	0.391	2.969
		Minimum	0.281	1.735	0.297	1.984
128x128		Maksimum	0.703	3.531	0.750	4.157
		Minimum	0.422	3.110	0.563	2.985

Dari Tabel IV diperoleh bahwa penambahan 1 share dan peningkatan ukuran citra dalam proses ekstraksi akan mengakibatkan perubahan waktu semakin besar baik untuk komputer 1 maupun komputer 2, baik waktu minimum maupun waktu maksimum. Metode BPCS mengalami perubahan waktu yang lebih besar dibandingkan dengan metode DE.

C. Hasil Pengujian Kapasitas

Pengujian ini dilakukan untuk mengetahui bagaimana pengaruh kapasitas share yang disisipkan terhadap kualitas amplop dengan melakukan perbandingan antara amplop yang sudah disisip share menggunakan metode DE atau BPCS dengan yang asli. Hasil pengujian dapat dilihat pada Tabel V berikut ini.

TABLE V. PENGUJIAN KAPASITAS AMPLOP

No	Ukuran Amplop	Jumlah Share (n)	PSNR	
			DE	BPCS
1	128 x 128	5	34.7002	39.7434
2		6	31.6093	39.6177
3		7	34.6645	39.7043
4		8	31.6982	39.7301
5		10	34.7106	39.7862
6	192 x 192	5	31.5164	40.2223
7		6	34.5924	40.1437
8		7	31.6625	40.0738
9		8	34.6829	40.0521
10		10	31.7318	40.0022
11	256 x 256	5	34.4905	39.5645
12		6	31.5741	39.5836
13		7	34.6237	39.6244
14		8	31.6505	39.6269
15	320 x 320	5	34.7153	39.3099
16		6	31.7509	39.4395
17		7	34.7462	39.5489
18	384 x 384	7	34.7889	39.3832
19		6	34.7716	39.3389
20		5	34.7162	39.3330
	Rata-Rata		34.673	39.694
	Simpangan Baku		0.00647	0.07755

Dari Tabel V dapat dilihat bahwa nilai rata-rata PSNR untuk DE adalah 34,673 dan untuk BPCS adalah 39,694.

D. Hasil Pengujian *Robustness*

Pengujian ini dilakukan untuk mengetahui ketangguhan (*robustness*) kedua metode untuk tetap menjaga *share* (informasi) yang ada di dalam amplop meskipun sudah diberi *noise* terhadap amplop tersebut dengan nilai probabilitas yang berbeda-beda yang semakin lama semakin besar. Hasil pengujian dapat dilihat pada Tabel VI berikut ini.

TABLE VI. HASIL PENGUJIAN KETANGGUHAN TERHADAP *NOISE*

No	Ukuran Citra	Nilai Prob	Digital Envelope		BPCS	
			PSNR Uniform	PSNR Salt&Pepper	PSNR Uniform	PSNR Salt&Pepper
1	128 x 128	0.001	Infinity	34.04705	Infinity	25.21136
2		0.002	Infinity	34.70564	Infinity	12.08299
3		0.003	Infinity	32.4758	Infinity	12.17244
4		0.004	Infinity	29.22174	Infinity	-
5		0.005	Infinity	28.40474	Infinity	-
6		0.006	Infinity	-	Infinity	-
7		0.007	Infinity	-	28.874	-
8		0.008	Infinity		17.3333	
9		0.009	Infinity		13.4671	
10		0.01	55.4008		13.4691	
11	192 x 192	0.001	Infinity	32.62428	Infinity	42.08101
12		0.002	Infinity	31.63245	Infinity	10.37015
13		0.003	Infinity	31.24195	Infinity	10.69
14		0.004	Infinity	29.36751	Infinity	-
15		0.005	Infinity	-	Infinity	-
16		0.006	Infinity	-	70.309	-
17		0.007	Infinity	-	47.6151	-
18		0.008	Infinity		40.1812	
19		0.009	85.5377		39.2856	
20		0.01	86.5268		27.2391	
21	256 x 256	0.001	Infinity	34.75489	Infinity	41.67282
22		0.002	Infinity	31.49686	Infinity	40.91116
23		0.003	Infinity	29.75772	Infinity	13.00263
24		0.004	Infinity	28.63566	Infinity	-
25		0.005	Infinity	-	Infinity	-
26		0.006	Infinity	-	Infinity	-
27		0.007	Infinity	-	Infinity	-
28		0.008	Infinity	-	Infinity	-
29		0.009	Infinity		Infinity	
30		0.01	Infinity		12.1833	

Berdasarkan PSNR yang dihasilkan pada Tabel VI, nilai probabilitas yang dapat ditoleransi untuk jenis *noise uniform* untuk ketiga ukuran citra adalah di bawah 0,01 dan untuk *noise salt & pepper* dengan ukuran citra 128x128 dan 192x192 adalah di bawah 0,003. Sedangkan untuk ukuran citra 256x256 adalah 0.002 pada metode DE. Pada metode BPCS nilai probabilitas yang dapat digunakan untuk *noise uniform* dengan ukuran citra 128x128 adalah di bawah 0.006 sedangkan untuk ukuran citra 192x192 dan 256x256 adalah di bawah 0,009. Kemudian untuk noise *salt & pepper* nilai probabilitas yang dapat digunakan di bawah 0,002 pada citra 256x256 serta di bawah 0.001 pada citra 128x128 dan 192x192.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian terhadap kedua metode pengamplopan diperoleh kesimpulan sebagai berikut:

1. Waktu eksekusi penyisipan dan ekstraksi DE jauh lebih efisien dibandingkan dengan BPCS. Penambahan jumlah *share* dan ukuran citra akan meningkatkan waktu eksekusi dimana perubahan waktu lebih cepat dialami oleh BPCS.
2. Fidelility BPCS sedikit lebih baik dibandingkan dengan DE
3. Metode DE lebih tangguh dibandingkan dengan BPCS saat menggunakan *noise uniform*, sementara untuk *noise salt & pepper* kedua metode mempunyai tingkat ketangguhan yang hampir sama.

Adapun saran yang dapat dilakukan untuk perbaikan berikutnya adalah:

1. Untuk mengingkatkan keamanan dan ketangguhan metode DE, beberapa kemungkinan perbaikan yang dapat dilakukan, seperti:
   a. Mengubah metode penyisipan sekuensial dengan metode yang lebih acak, misalnya dengan menerapkan generator modulo atau pengacakan lainnya sehingga lebih sulit bagi penyerang mendapatkan data yang disembunyikan
   b. Menerapkan metode penyisipan *parity checker* sehingga pengubahan piksel amplop hanya dilakukan dengan aturan *parity* genap atau ganjil
2. Untuk metode BPCS perlu dipikirkan cara meningkatkan waktu eksekusinya karena dari sisi keamanan metode ini lebih baik

Referensi

[1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology - Eurocrypt'94*, pp. 1-12, 1995.

[2] S. Kandar and A. Maiti, "Variable length key based visual cryptography scheme for color image using random number", *International Journal of Computer Application*, vol. 19, pp. 35-40, 2011.

[3] A. Bhakta, S. Maiti, R. Das and S. Dutta, "An approach of visual cryptography scheme by cumulative image encryption technique using image-key encryption, bit-sieved operation and k-n secret scheme", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 4, pp. 20-23, 2013.

[4] H. Gao, Y. Zhang, S. Liang and D. Li, "A new chaotic algorithm for image encryption", *Chaos Solutions and Fractal*, vol. 29, pp. 393-399, 2006.

[5] A. Kawagauchi and R. Eason, "Principle and application of bpcs-steganography", *Proc. SPIE*, vol. 3529, pp. 464-473, 1998.

[6] M.Ramani, E. Prasad and S. Varadarajan, "Steganography using BPCS to the integer wavelet transformed image", *International Journal of Computer Science and Network Security*, vol. 7(7), pp. 293-302, 2007.

[7] R. Das, S. Dutta and S. Kuila, "Approach of visual cryptography scheme for color image by cumulative encryption using image partitioning, text key encryption, image key encryption & digital enveloping", *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, pp. 1341-1349, 2013.

[8] S. Samanta, P. Mondol, R. Das and S. Dutta, "An approach of visual cryptography scheme for color image by using even and odd block based digital enveloping", *International Journal of Innovative Technology & Adaptive Management (IJITAM)*, vol. 1, 2014.