Implementasi Kripto-Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital

Paulus Lucky Tirma Irawan, D.J. Djoko H. Santjojo, M. Sarosa

***Abstrak*—In this research, cryptography of SALSA20 stream cipher technique combined with BPCS steganography technique was used to enhance the security layer in mobile communication. SALSA20 technique has been proven as one of the best stream cipher algorithm candidate according to eSTREAM portfolio report in 2012. The combination of SALSA cryptography and BPCS steganography technique can provide more security layer of digital image data as the research objective.**

The results from this research showed that combination of SALSA20 and BPCS technique need average time of 19.400s for the encryption and 21.900s for decryption process. The average memory (RAM) usage of these two technique is about 23.354 MB/s for the encryption process and 36.057 MB/s for the decryption. The analysis of component MSE and PSNR show a good result with value of 16.21259 dB for the MSE component and +44.08686 dB for the PSNR, with color contrast intensity distribution of the output image nearly identical to the original cover image.

***Keywords*—BPCS, Cryptography, SALSA20, Steganography.**

***Abstrak*— Dari teknologi surat elektronik (e-mail), komunikasi selular, keamanan akses laman web, hingga sistem pembayaran online, kriptologi memegang peranan penting. Berdasarkan penelitian, ditemukan fakta bahwa telah terjadi peningkatan ancaman secara signifikan khususnya pada perangkat bergerak. Beberapa literatur pustaka menjelaskan secara rinci bahwa pencurian data atau informasi masih menjadi kasus dengan total persentase kejadian yang sangat tinggi saat ini.**

Dalam penelitian ini akan digunakan kombinasi teknik kriptografi cipher aliran SALSA20 dan teknik steganografi BPCS. Teknik kriptografi SALSA20 telah terpilih sebagai salah satu kandidat algoritma kriptografi cipher aliran terbaik menurut eSTREAM portfolio tahun 2012. Implementasi kombinasi kedua teknik kriptografi dan steganografi ini bertujuan untuk memberikan tingkat keamanan yang baik terhadap data citra digital yang menjadi objek penelitian.

Berdasarkan hasil pengujian yang sudah dilakukan Hybrid teknik kriptografi Salsa20 dan teknik steganografi BPCS membutuhkan rata-rata waktu 19,400 detik untuk lama proses enkripsi dan 21,900 detik untuk proses dekripsinya. Dalam implementasinya kedua teknik ini, rerata penggunaan memori RAM perangkat adalah sebesar 23,354 MB/s untuk proses enkripsi dan 36,057 MB/s untuk proses dekripsinya. Dari hasil analisa pengujian yang sudah dilakukan didapatkan rerata nilai komponen MSE sebesar 16,21259 dB, dan nilai PSNR mencapai +44,08686 dB, dengan sebaran intensitas citra keluaran yang hampir serupa dengan citra cover aslinya.

***Kata Kunci*—BPCS, Kriptografi, SALSA20, Steganografi.**

Paulus Lucky Tirma Irawan adalah Dosen Universitas Ma Chung dan mahasiswa Program Magister Teknik Elektro Universitas Brawijaya, Malang, Indonesia, phone: 085959823367; email lockey.irawan@gmail.com

Djoko HS adalah Dosen Program Studi Geofisika, Jurusan Fisika, FMIPA Universitas Brawijaya, Malang, Indonesia, phone: 081555828240; email: santjojo@fizzy.murdoch.edu.au

M. Sarosa adalah Dosen Program Studi Teknik Elektro, Politeknik Negeri Malang, Indonesia, phone: 08122440326, email: rmsarosa@gmail.com

I. PENDAHULUAN

KRIPTOLOGI membantu para penyedia jasa layanan dalam menyediakan komponen akuntabilitas, kejujuran, akurasi dan kerahasiaan kepada para pengguna terhadap data atau informasi yang menjadi komponen penting dalam sebuah sistem informasi. Melalui teknik-teknik pengamanan data yang terdapat dalam kriptologi, kita dapat mencegah terjadinya penyalahgunaan dalam sistem komersial elektronik, memastikan validitas dari sebuah transaksi finansial yang telah dilakukan, hingga membuktikan kepemilikan asli maupun memberikan perlindungan terhadap privasi penggunanya.

Dalam sebuah laporan penelitian yang dilakukan oleh Webroot berjudul *The Webroot Mobile Threat Report: An Overview of The Risks and Trends of The Mobile Space* tahun 2014 ini, dikemukakan sebuah fakta bahwa telah terjadi peningkatan ancaman sebanyak 384% dibandingkan dengan data yang pada tahun 2012 yang lalu [1]. Sementara dalam *Symantec Internet Security Threat Report 2014 Volume 19: Mobile Threat Classifications* dikemukakan bahwa kasus pencurian data atau informasi digital masih menjadi salah satu ancaman dengan total persentase yang paling tinggi [2]. Rentannya tingkat keamanan data yang ada saat ini terutama pada media perangkat bergerak menjadi alasan utama dibutuhkannya sebuah metode atau teknik khusus yang dapat menjadi alternatif solusi terhadap masalah ancaman yang terjadi saat ini.

Dalam penelitian ini akan diimplementasikan teknik kriptografi cipher aliran SALSA20 yang telah terbukti sesuai untuk diterapkan pada perangkat dengan spesifikasi terbatas seperti perangkat bergerak berdasarkan spesifikasi eSTREAM *portfolio* 2012 [3]. Kombinasi teknik kriptografi SALSA20 dan teknik steganografi BPCS diharapkan dapat memberikan sebuah layer keamanan pada data atau informasi pengguna pada komunikasi data perangkat bergerak. Serangkaian uji analisa akan dilakukan untuk melihat sejauh mana performansi serta kualitas yang dihasilkan dari penggabungan teknik SALSA20 dan BPCS ini dengan memperhatikan prameter MSE, PSNR, serta data grafik analisa histogram.

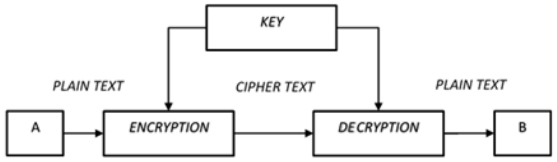
II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi secara umum berkaitan erat dengan kerahasiaan atau keamanan pesan (*privacy*), seperti salah satu definisi terkait tentang kriptografi menyatakan bahwa kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Namun seiring perkembangan jaman, pemahaman kriptografi lebih dari hanya sekedar permasalahan *privacy* semata, namun juga dikaitkan dengan beberapa aspek keamanan lainnya seperti *data integrity*, *authentication*, dan *non-repudiation* [4].

- Konsep Dasar Kriptografi Kunci Simetris

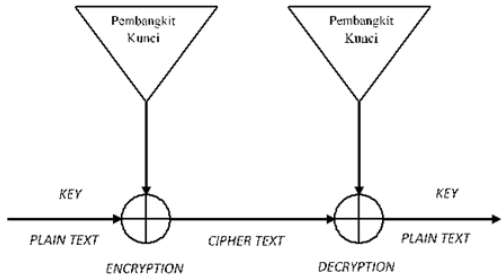
Kriptografi kunci simetris merupakan kriptografi yang dalam proses enkripsi dan dekripsinya hanya menggunakan satu buah kunci yang sama. Kelebihan dari algoritma kriptografi kunci simetris ini adalah waktu proses enkripsi dan dekripsi datanya yang membutuhkan waktu relatif singkat sehingga algoritma ini sangat sesuai untuk diterapkan pada sistem komunikasi digital.



Gambar 1. Proses Kriptografi Kunci Simetris

- Konsep Dasar Kriptografi Cipher Aliran

Pada algoritma kriptografi cipher aliran, masukan diterima dalam bentuk aliran bit. Proses enkripsi dan dekripsinya dilakukan pada aliran bit dengan memproses bit satu per satu. Secara umum cipher aliran membangkitkan aliran kunci dari kunci yang dimasukkan oleh pengguna. Ketika aliran kunci telah dibangkitkan, maka proses enkripsi dan dekripsi dilakukan melalui operasi XOR antara bit aliran kunci dengan bit *plaintext* atau *ciphertext*.



Gambar 2. Proses Kriptografi Cipher Aliran

- Kriptografi SALSA20

Salsa20 merupakan algoritma kriptografi berbasis cipher aliran yang dikembangkan oleh Daniel J. Bernstein pada tahun 2005 dan termasuk ke dalam salah satu kandidat eSTREAM Project tahun 2012 [5][6].

Secara umum algoritma kriptografi Salsa20 membangkitkan aliran kunci dari kunci masukan, kemudian melakukan operasi XOR antara aliran kunci dengan *cipher-text* atau *plain-text*. Algoritma Salsa20 menerima input berupa 32 bytes *key*, 8 byte *nonce*, 8 byte *block counter* (maksimum). Setelah dilakukan proses pembangkitan aliran kunci kemudian dilakukan operasi XOR antara aliran kunci dan *plain-text*. Besar aliran kunci yang dihasilkan oleh SALSA20 adalah 64 byte.

B. Steganografi

Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa terdapat suatu pesan rahasia [4]. Namun, kini istilah steganografi sudah semakin meluas maknanya, termasuk penyembunyian data digital dalam file-file komputer.

- Konsep Dasar Sistem Kerja Steganografi

Teknik steganografi memiliki banyak sekali metode komunikasi yang dapat digunakan untuk menyembunyikan sebuah pesan rahasia, biasanya berupa teks atau gambar, ke dalam media file lainnya, seperti teks, gambar hingga jenis file audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur file mulanya.

Dalam penerapannya, metode steganografi kebanyakan diselesaikan dengan melakukan perubahan-perubahan kecil terhadap data digital yang bertindak sebagai media perantaranya. Perubahan ini akan sangat bergantung terhadap kunci (sama halnya dengan algoritma kriptografi) dan pesan yang akan disembunyikan nantinya. Di sisi penerima, pesan rahasia yang terdapat di dalamnya dapat diungkap dengan jalan memasukkan kunci yang tepat ke dalam algoritma steganografi yang digunakan.

- Kriteria Teknik Steganografi

Terdapat beberapa kriteria yang harus diperhatikan dalam steganografi, meliputi *interceptibility fidelity*, dan *recovery* [4].

- Bit-Plane Complexity Segmentation

Bit-Plane Complexity Segmentation (BPCS) adalah salah satu teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1997 untuk mengatasi kekurangan yang muncul pada beberapa teknik steganografi konvensional seperti *Least Significant Bit* (LSB), teknik *transform embedding*, dan teknik *masking perceptual* [7].

Berikut adalah langkah-langkah yang dilakukan pada algoritma BPCS saat menyisipkan data:

1. Mengubah cover image dari sistem PBC (*Pure-Binary Coding System*) menjadi sistem CGC (*Canonical Gray Coding System*). Sebelumnya, gambar tersebut dibagi-bagi terlebih dahulu menjadi bit-plane. Setiap bit-plane mewakili bit dari setiap piksel.
2. Segmentasi setiap bit-plane pada *cover image* menjadi *informative* dan *noise-like region* menggunakan nilai batas/threshold ($\alpha 0$).
3. Bagi setiap byte pada data rahasia menjadi blok-blok (S).
4. Jika blok (S) tidak lebih kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S* yang lebih kompleks.
5. Sisipkan setiap blok data rahasia ke bit-plane yang merupakan *noise-like region*. Kemudian simpan data konjugasi pada "*conjugation map*".
6. Sisipkan juga pemetaan konjugasi yang telah dibuat

C. Pengujian Kualitas Citra Digital

Pengukuran kualitas citra hasil keluaran dari penggabungan kedua teknik kriptografi cipher aliran Salsa20 dan teknik steganografi *Bit-Plane Complexity Segmentation* (BPCS) dilakukan menggunakan perhitungan matematis terhadap besaran nilai parameter MSE (*Mean Square Error*) dan PSNR (*Peak-Signal-to-Noise Ratio*). Untuk mendukung pengujian ini juga akan dilakukan uji komparasi terhadap citra hasil keluaran (*stego-image*) menggunakan analisa histogram.

- MSE (*Mean Square Error*)

Mean Square error merupakan parameter yang menunjukkan tingkat kesalahan piksel-piksel citra hasil pemrosesan signal (*stego image*), terhadap citra asli (*media cover*). Semakin kecil nilai MSE yang didapatkan maka kualitas citra keluaran akan semakin baik atau secara gamblang dapat dikatakan semakin mendekati citra aslinya. Nilai dari pada parameter MSE ini dinyatakan dalam satuan desibel (dB).

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left|\left(f(x,y)-g(x,y)\right)^2\right| \quad \text{.....(1)}$$

- PSNR (*Peak-Signal-to-Noise Ratio*)

PSNR atau *Peak-Signal-to-Noise Ratio* merupakan parameter besaran yang menunjukkan rasio tingkat toleransi *noise* tertentu terhadap banyaknya *noise* pada suatu piksel citra. *Noise* yang dimaksudkan di sini adalah kerusakan piksel pada bagian tertentu dalam sebuah citra sehingga

mempengaruhi kualitas dari pada piksel tersebut. Dengan kata lain PSNR menunjukkan nilai kualitas suatu piksel citra. Persamaan untuk menghitung nilai komponen PSNR dari sebuah citra dapat dirumuskan sebagai berikut.

$$PSNR = {}^{20}\log 10\left(\frac{255}{\sqrt{MSE}}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

PSNR yang lebih tinggi menunjukkan bahwa kualitas citra hasil keluaran lebih baik atau secara gamblang dapat dikatakan menyerupai citra aslinya. Nilai parameter PSNR ini dinyatakan dalam satuan desibel (dB). Nilai PSNR yang baik untuk citra adalah lebih besar dari 30 dB.

- Analisa Histogram

Analisa histogram ditujukan untuk mengetahui sebaran intensitas piksel dari sebuah citra digital yang memudahkan untuk melakukan penilaian melalui beberapa komponen dasar, meliputi komponen puncak histogram, lebar puncak histogram, rentang kontras citra, serta kondisi pencahayaan sebuah citra digital.

III. METODOLOGI

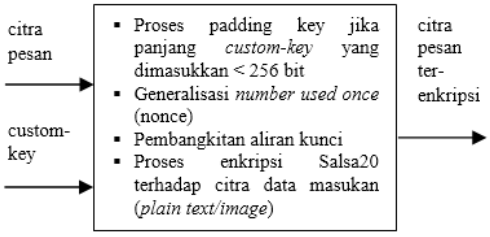
Pengamanan data citra digital (.BMP) diawali dengan proses enkripsi citra pesan rahasia menggunakan teknik kriptografi SALSA20 dengan sebuah kunci sebuah string tertentu dengan panjang maksimum 32 karakter untuk menghasilkan citra pesan rahasia terenkripsi. Citra pesan ini kemudian akan disematkan ke dalam sebuah citra cover (*cover image*) menggunakan teknik steganografi BPCS dengan nilai threshold sebesar 0,4 untuk menghasilkan citra stego (*stego image*) yang sudah berisi pesan rahasia terenkripsi di dalamnya.

Teknik Kriptografi SALSA20

Algoritma kriptografi Salsa20 memiliki cara kerja yang serupa dengan algoritma-algoritma kriptografi lainnya secara umum. Prosesnya terbagi ke dalam tiga bagian besar, yakni proses inisialisasi (*input*), proses enkripsi/dekripsi Salsa20, rekonstruksi hasil keluaran (*output*).

Alur kerja teknik kriptografi SALSA20 ini dapat dijelaskan sebagai berikut.

1. Proses inisialisasi pembangkitan aliran kunci yang dibangun dari 3 komponen utama, yakni citra pesan yang akan dilakukan proses enkripsi (*plain image*), *custom-key*, serta komponen *nonce* yang dibangkitkan secara acak.
2. Validasi panjang *custom-key* yang dimasukkan. Jika panjang *custom-key* yang dimasukkan kurang dari 32 karakter maka akan dilakukan proses *padding*.
3. Pembangkitan bilangan acak untuk menghasilkan komponen *nonce*.
4. Operasi enkripsi SALSA20 dilakukan dengan melakukan operasi XOR antara aliran kunci yang sudah dibangkitkan dengan deretan kode biner citra pesan (*plain image*) untuk menghasilkan citra pesan terenkripsi (*cipher image*) dalam deretan kode biner.

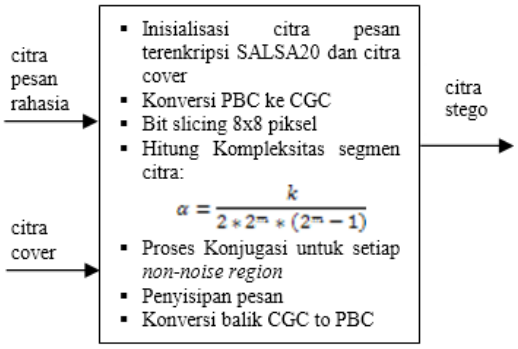


Gambar 3. Alur Proses SALSA20

Teknik Steganografi BPCS

Fase teknik steganografi BPCS juga terbagi ke dalam 3 bagian besar, dimulai dari proses inisialisasi data masukan berupa citra pesan terenkripsi SALSA20, rangkaian sub-proses dari teknik BPCS itu sendiri, hingga fase final, dimana akan diperoleh hasil keluaran berupa sebuah citra stego (*stego image*) dengan pesan rahasia di dalamnya. Berikut alur kerja dari pada algoritma BPCS [8][9].

1. Tahapan inisialisasi dari proses steganografi diawali dengan masukan citra pesan rahasia dan citra cover yang bertindak sebagai wadah penampung (*vessel image*) pesan rahasia tersebut.
2. Konversi sistem citra cover dari sistem PBC (*Pure Binnary Code*) ke dalam bentuk sistem CGC (*Canocical Gray Code*).
3. Pembagian citra cover ke dalam segmen-segmen citra berukuran 8x8 piksel (*bit slicing*) untuk masing-masing citra citra pesan dan citra cover yang digunakan untuk kemudian dilakukan analisa wilayah informasi (*informatif region*) dan wilayah *noise* (*noise-like region*).
4. Perhitungan kompleksitas segmen citra dengan cara melakukan perbandingan antara nilai kompleksitas setiap segmen citra dengan nilai threshold yang telah ditetapkan sebelumnya (threshold=0,4).
5. Lakukan proses konjugasi untuk setiap segmen citra pesan rahasia yang tidak termasuk *noise region* untuk menambah nilai kompleksitas segmen citra tersebut.
6. Proses penyisipan pesan rahasia ke dalam segmen *noise* (*noise-like region*) citra cover.
7. Konversi balik citra cover yang sudah disisipkan pesan rahasia ke dalam sistem PBC untuk menghasilkan citra stego yang diinginkan (*stego-image*).



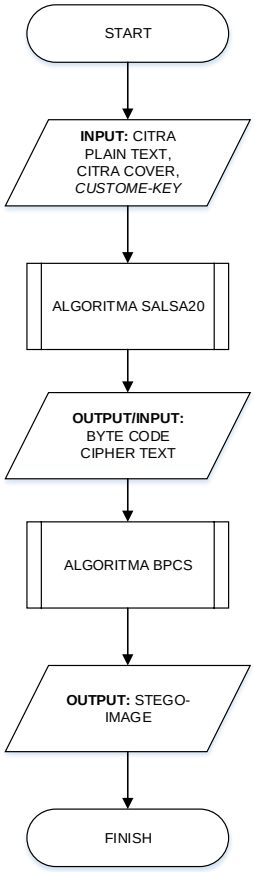
Gambar 4. Alur Proses BPCS

Penggabungan Teknik SALSA20 dan BPCS

Integrasi dari kedua teknik kriptologi, yakni teknik kriptografi cipher aliran Salsa20 dan steganografi Bit-Plane Complexity Segmentation ini merupakan satu rangkaian proses yang tidak terputus yang diawali dengan proses pengacakan pesan rahasia berupa citra digital dengan teknik kriptografi Salsa20, yang kemudian dilanjutkan dengan proses penyisipan ke dalam sebuah media cover atau juga biasa disebut *vessel image* menggunakan teknik steganografi BPCS. Hasil keluaran dari proses ini adalah sebuah citra stego dengan pesan rahasia terenkripsi.

Citra stego yang sudah dihasilkan pada proses enkripsi-penyisipan akan digunakan kembali pada proses dekripsi pesan rahasia (proses dekripsi-ekstraksi pesan) bersama dengan parameter *custom-key* untuk kemudian dilakukan proses pengambilan pesan rahasia yang sudah disisipkan di dalam citra penampung (*vessel image*). Jika salah satu

komponen masukan tidak sesuai maka proses ini tidak dapat dilaksanakan.



Gambar 5. Diagram Alir Proses Enkripsi Hybrid Teknik Kriptografi Salsa20 dan Teknik Steganografi BPCS

Langkah-langkah penggabungan dari kedua teknik pengamanan data seperti yang tertera pada Gambar 5 dapat dijelaskan sebagai berikut.

1. Alur kerja sistem aplikasi ini diawali dengan penentuan data masukan (*input*) yang bertindak sebagai pesan rahasia (*secret message*) berupa citra digital yang akan dikenakan proses kriptografi Salsa20 dan steganografi *Bit-Plane Complexity Segmentation*. Data masukan yang akan digunakan dalam penelitian ini diunduh dari sebuah situs resmi milik University of Southern California, Signal and Image Processing Institute.
2. Dari data masukan yang sudah diberikan ke dalam sistem, kemudian akan dilakukan proses pengacakan data menggunakan teknik kriptografi cipher aliran Salsa20 dengan terlebih dahulu memasukkan kunci kriptografi (*custom key*). Data masukan yang digunakan sebagai kunci dalam penelitian ini adalah serangkaian karakter dengan panjang 32 karakter atau sekitar 32 bytes (256 bits) sesuai dengan kriteria masukan dari algoritma Salsa20 itu sendiri. Jika panjang kunci tidak memenuhi kriteria, maka akan dilakukan proses penambahan bit kunci (*padding*) sehingga data kunci menjadi valid.
3. Setelah dilakukan proses kriptografi Salsa20, data keluaran (*cipher text*) dari proses kriptografi ini kemudian akan dilanjutkan dengan proses penyematan ke dalam sebuah media cover (*cover image*) menggunakan teknik steganografi *Bit-Plane Complexity Segmentation*. Media cover yang digunakan dalam penelitian ini masih menggunakan basis data yang sama seperti pada data masukan sistem pada proses pertama (*secret message*).
4. Sampai tahap ini, proses penggabungan teknik kriptografi cipher aliran Salsa20 dan teknik steganografi BPCS sudah bisa dikatakan selesai dengan didapatkannya hasil keluaran (*output*) berupa citra stego (stego image), yakni data citra media (*cover image*) yang sudah disemati pesan rahasia terenkripsi (*secret message*).

Tahapan selanjutnya memiliki alur proses yang berkebalikan dengan proses sebelumnya, karena pada tahapan ini pesan rahasia yang sudah berhasil disematkan pada media cover akan diekstrasi untuk mendapatkan pesan aslinya menggunakan proses dekripsi Steganografi BPCS dan dekripsi Salsa20. Indikator keberhasilan dari pada tahap dekripsi ini adalah didapatkannya pesan asli yang sebenarnya tanpa mengalami perubahan.

Tahapan akhir proses penelitian yang akan dilakukan ini berujung pada analisa terhadap performansi yang diberikan dari pada penggabungan kedua teknik kriptologi, yakni teknik kriptografi cipher aliran Salsa20 dan teknik steganografi *Bit-Plane Complexity Segmentation* (BPCS). Analisa performansi dilakukan dengan membandingkan citra hasil keluaran (*output/stego image*) dengan media cover (*cover image*) berdasarkan nilai yang diperoleh menggunakan perhitungan nilai MSE (*Mean Squared Error*), PSNR (*Peak-Signal-to-Noise Ratio*), dan analisa histrogram.

IV. HASIL DAN PEMBAHASAN

Pengujian yang telah dilakukan meliputi pengujian citra hasil keluaran dari proses enkripsi dan dekripsi dari penggabungan teknik kriptografi cipher aliran Salsa20 dan teknik steganografi BPCS, analisa tingkat performansi dari sistem yang sudah dikembangkang melalui analisa parameter waktu proses enkripsi dan dekripsi pesan (detik), rerata total penggunaan memori (RAM) dari perangkat Android, serta analisa performansi kualitas citra keluaran yang dihasilkan dari proses hybrid dua teknik kriptografi SALSA20 dan steganografi BPCS yang diketahui dari parameter MSE, PSNR dan melalui analisa histogram. Pengujian dilakukan terhadap 40 data citra sampel pengujian (.BMP).

Dari hasil pengujian tersebut yang tertera pada Tabel I, didapatkan nilai rerata waktu proses enkripsi untuk citra berukuran 128x128 piksel dengan citra cover berukuran 256x256 piksel adalah sebesar 19,400 detik sementara untuk proses dekripsi pesan rahasia membutuhkan waktu sebesar 21,900 detik. Sementara rerata penggunaan memori RAM perangkat pengujian dapat dilihat pada tabel II selanjutnya.

TABEL I
WAKTU PROSES ENKRIPSI-DEKRIPSI SALSA20 & BPCS

Citra Pesan (.bmp)	Citra Cover (.bmp)	Lama Waktu Proses Enkripsi (detik)	Lama Waktu Proses Dekripsi (detik)
image1	Image11	12	20
image2	Image12	9	24
image3	Image13	6	27
image4	Image14	8	20
image5	Image16	8	24
image6	Image16	17	20
image7	Image17	5	20
Image8	Image18	7	19
Image9	Image19	40	25
Image10	Image20	82	20

Sementara Tabel II menunjukkan total pemakaian memori RAM perangkat untuk proses hybrid teknik kriptografi

SALSA20 dan teknik steganografi BPCS. Berdasarkan data hasil pengujian diketahui pemakaian memori RAM perangkat pengujian untuk proses enkripsi pesan citra digital berukuran 128x128 piksel dengan citra cover berukuran 256x256 piksel adalah sebesar 23,354 MB/s dan untuk proses dekripsinya sebesar 36,057 MB/s. Hasil pengujian yang tertera pada Tabel II menjadi indikator penilaian terhadap komponen performansi yang dihasilkan dari proses penggabungan algoritma kriptografi cipher aliran SALSA20 dan algoritma steganografi *Bit-Plane Complexity Segmentation* (BPCS). Hasil pengujian didapatkan dengan menggunakan perangkat pengujian perangkat genggam dengan spesifikasi perangkat keras, yakni komponen CPU Quad-core 1,4 GHz dengan kapasitas RAM perangkat 1 GByte.

TABEL II
WAKTU PROSES ENKRIPSI-DEKRIPSI SALSA20 & BPCS

Citra Pesan	Citra Cover	Penggunaan Memori Proses Enkripsi (MB/s)	Penggunaan Memori Proses Dekripsi (MB/s)
image1	image11	16,30	29,42
image2	Image11	27,20	39,10
Image3	Image11	35,59	48,91
Image4	Image11	15,51	27,62
Image5	Image11	28,05	39,41
Image6	Image11	40,18	52,80
Image7	Image11	12,60	26,57
Image8	Image11	26,06	39,52
Image9	Image11	14,11	27,54
Image10	Image11	26,70	38,94

Tabel III menunjukkan sampel hasil perbandingan kualitas citra pesan hasil proses ekstraksi pesan pada proses hybrid teknik kriptografi SALSA20 dan BPCS dengan citra pesan asli sebelum dilakukan proses enkripsi-penyisipan pesan. Dari hasil pengujian didapatkan nilai parameter tak terhingga (∞) dan nilai parameter MSE 0.000 dB yang menunjukkan bahwa kualitas pesan ekstraksi adalah sangat baik, identik dengan citra pesan aslinya dan tidak mengalami kerusakan dalam proses penyisipannya. Hasil yang ditunjukkan pada Tabel III menjadi indikator penting untuk menilai keberhasilan dari sebuah teknik penyisipan data (steganografi) yang digunakan, yakni teknik steganografi BPCS itu sendiri.

TABEL III
HASIL PERBANDINGAN KUALITAS CITRA KELUARAN

Citra Pesan Asli	Citra Pesan Ekstraksi	Hasil Analisa Parameter PSNR (dB)	Hasil Analisa Prameter MSE (dB)
(image10.bmp)	(testing10.bmp)	∞	0.000

Tabel IV menunjukkan data hasil pengujian terhadap parameter MSE terhadap citra cover asli sebelum dilakukan proses penyisipan pesan dengan citra cover *embeded* yang sudah disisipkan pesan di dalamnya. Berdasarkan hasil pengujian didapatkan rerata nilai MSE sebesar 16,21259 dB. Rerata nilai MSE yang cukup kecil menunjukkan bahwa citra penampung yang sudah disematkan pesan rahasia di dalamnya tidak mengalami banyak kerusakan piksel atau juga dapat dikatakan perubahan yang terjadi pada citra penampung hampir tidak dapat disadari secara kasat mata.

TABEL IV
DATA ANALISA PARAMETER MSE

Citra Cover Asli (.BMP)	Citra Cover Embeded (.BMP)	Nilai Parameter MSE (dB)
image11.bmp	testing-1.bmp	13,78586
image12.bmp	testing-2.bmp	27,26511
image13.bmp	testing-3.bmp	16,06148
image14.bmp	testing-4.bmp	13,62811
image16.bmp	testing-5.bmp	10,17847
image16.bmp	testing-6.bmp	10,17847
image17.bmp	testing-7.bmp	0,07062
image18.bmp	testing-8.bmp	0,00183
image19.bmp	testing-9.bmp	0,48233
image20.bmp	testing-10.bmp	22,39064

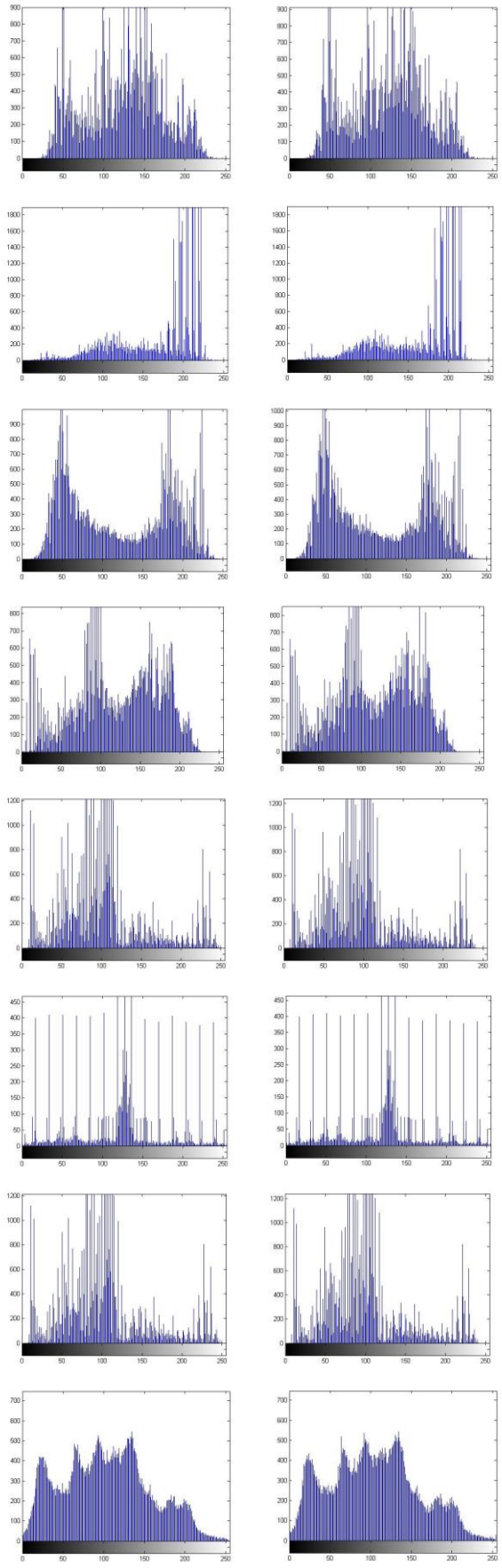
Tabel V memberikan data analisa pengujian terhadap parameter PSNR terhadap citra cover asli dan citra cover *embeded*. Berdasarkan data yang didapatkan dari proses pengujian, diketahui kualitas citra cover *embeded* yang dihasilkan dari proses hybrid teknik kriptografi SALSA20 dan teknik steganografi BPCS adalah baik, yakni dengan rerata nilai parameter PSNR mencapai lebih dari 30,000 dB (+ 44,08686 dB).

TABEL V
DATA ANALISA PARAMETER PSNR

Citra Cover Asli (.BMP)	Citra Cover Embeded (.BMP)	Nilai Parameter PSNR (dB)
image11.bmp	testing-1.bmp	+36,77046
image12.bmp	testing-2.bmp	+33,78586
image13.bmp	testing-3.bmp	+36,10694
image14.bmp	testing-4.bmp	+36,82044
image16.bmp	testing-5.bmp	+38,08798
image16.bmp	testing-6.bmp	+38,08798
image17.bmp	testing-7.bmp	+59,67567
image18.bmp	testing-8.bmp	+75,53779
image19.bmp	testing-9.bmp	+51,33135
image20.bmp	testing-10.bmp	+34,66413

Bentuk pengujian selanjutnya merupakan uji analisa histogram untuk mengetahui representasi grafis distribusi warna serta intensitas piksel dari sebagian atau keseluruhan sebuah citra digital. Berdasarkan pengujian yang sudah dilakukan menggunakan perangkat bantuan Matlab, dapat diketahui beberapa hal menarik meliputi komponen puncak histogram, lebar puncak, serta kondisi pencahayaan dari sebuah citra digital. Pengujian menggunakan analisa histogram digunakan untuk mengetahui kesamaan sebaran warna dari citra yang dibandingkan dalam derajat intensitas keabuan. Hasil analisa ini dapat digunakan untuk mengetahui kesamaan pola warna yang ada pada gambar yang dibandingkan, baik citra penampung sebelum dilakukan proses enkripsi-penyisipan pesan dengan citra keluaran (*stego-image*) yang merupakan citra keluaran yang telah berisi pesan citra rahasia.

Pada Gambar 6 dapat dilihat representasi hasil analisa histogram dari citra cover asli dan citra cover *embeded*. Berdasarkan data pengujian yang didapat, sesuai dengan data hasil pengujian pada parameter MSE dan PSNR sebelumnya diketahui bahwa baik citra cover sebelum disematkan pesan rahasia dengan citra cover yang sudah disematkan pesan rahasia (*stego-image*) memiliki karakteristik yang nyaris serupa dilihat dari lebar puncak, rentang kontras serta sebaran intensitas piksel dari kedua tersebut yang secara kasat mata sulit untuk dibedakan atau nyaris identik.



Gambar 6. Perbandingan Grafik Analisa Histogram Citra Cover Asli (kiri) dan Citra Cover *Embeded* (kanan)

V. KESIMPULAN

Berdasarkan data-data hasil pengujian tersebut, dapat ditarik beberapa kesimpulan terkait dengan penerapan teknik kriptografi cipher aliran Salsa20 dan teknik steganografi BPCS sebagai berikut:

1. Hybrid teknik kriptografi Salsa20 dan teknik steganografi BPCS telah berhasil dilakukan dengan baik. Hal ini dapat dilihat pada keberhasilan proses enkripsi-penyisipan pesan serta proses dekripsi-pembongkaran pesan rahasia yang mencapai 100%, dimana citra yang disisipkan adalah identik sama dengan citra yang diekstrak dari sebuah cita stego sebelumnya.
2. Hybrid teknik kriptografi Salsa20 dan teknik steganografi BPCS membutuhkan waktu yang cukup lama untuk proses enkripsi dan dekripsi pada objek citra berukuran 128x128 dengan lebar citra cover 256x256, yakni mencapai 19,400 detik untuk lama proses enkripsi dan 21,900 detik untuk lama proses dekripsi. Hal ini tentunya harus menjadi perhatian utama mengingat citra pengujian terbilang kecil.
3. Hybrid teknik kriptografi Salsa20 dan teknik steganografi BPCS juga membutuhkan penggunaan memori RAM perangkat yang terbilang cukup besar, yakni mencapai nilai 23,354 MB/s untuk proses enkripsi dan 36,057 MB/s untuk proses dekripsinya.
4. Berdasarkan hasil pengujian terhadap tiga komponen citra digital yang meliputi nilai MSE sebesar 16,21259, dan nilai PSNR mencapai +44,08686 dB. Sementara dari analisa grafik histogram dapat dilihat bahwa sebaran intensitas piksel citra cover yang sudah disisipkan pesan rahasia dengan yang belum bisa dikatakan identik serupa.

Pada penelitian berikutnya diharapkan dapat diujicobakan teknik kriptografi cipher aliran kandidat eSTREAM portfolio lainnya, seperti TRIVUM dan GRAIN v.1 yang juga terbukti memiliki performansi kerja yang baik.

DAFTAR PUSTAKA

[1] Webroot. (4 Februari 2014). Webroot Mobile Threat Report: An Overview of The Risks and Trends of The Mobile Space [Online]. Tersedia:http://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf.

[2] Symantec. Mobile Threat Classifications. Symantec Internet Security Threat Report Vol. 19. Agustus, 2014.

[3] eCRYPT. (12 Oktober 2012). D. SYM. 10 The eSTREAM Portfolio in 2012 [Online]. Tersedia:http://www.ecrypt.eu.org/documents/D.SYM.10-v1.pdf.

[4] Munir, Rinaldi. *Kriptografi*. Bandung: Informatika, 2006.

[5] Bernstein, Daniel J. (10 Januari2014). Salsa20 Spesification. Tersedia: http://cr.yp.to/snuffle/spec.pdf

[6] Meiser, G. et al. Efficient implementation of eSTREAM ciphers on 8-bit AVR microcontrollers. IEEE Industrial Embedded Systems SIES 2008, p58-66.

[7] Jolfaei, Alireza., dan Mirghadri. Survey: Image Encryption Using Salsa20. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 5. IJCSI Doolar Lane, Mahebourg, 2010.

[8] Kawaguchi, eiji dan Eason, Richard O. Principle and Applications of BPCS-Steganography. Proc. SPIE 3528, Multimedia Systems and Applications, 464, 1998.

[9] Patel, V.J. dan Soni, N.R. Uncompressed Image Steganography Using BPCS: Survey and Analysis. IOSR Journal of Computer Engineering (IOSR-JCE), 2013, vol. 15, Issue 4.