KOMBINASI STEGANOGRAFI *BIT PLANE COMPLEXITY SEGMENTATION* (BPCS) DAN KRIPTOGRAFI *DATA ENCRYPTION STANDARD* (DES) UNTUK PENYISIPAN PESAN TEKS PADA CITRA *BITMAP GRAYSCALE* 8 BIT

Paulus Klau [1], Derwin Rony Sina [2], Yelly Y.Nabuasa [3]
[1,2,3] Jurusan Ilmu Komputer, Fakultas Sains dan Teknik, Universitas Nusa Cendana

INTISARI

***Bit Plane Complexity Segmentation* (BPCS) merupakan metode steganografi yang menggunakan ketidakmampuan penglihatan manusia dalam menginterpretasi pola biner yang rumit. *Data Encryption Standard* (DES) merupakan algoritma kriptografi yang bersifat *cipher block* dan mengubah data masukan menjadi blok-blok 64 bit dan kemudian menggunakan kunci enkripsi sebesar 56 bit. Dengan mengkombinasikan algoritma steganografi dan kriptografi akan meningkatkan kualitas keamanan data. Pada penelitian ini kombinasi BPCS dan DES dilakukan dengan menyisipkan pesan teks ke dalam citra *bitmap*. Pesan teks yang disisipkan dibatasi maksimal 248 karakter dengan panjang kunci harus 16 karakter dalam format *heksadesimal*. Hasil yang diperoleh dari pengujian sistem ini dengan citra uji sebanyak 30 citra *bitmap* yaitu pesan yang disisipkan dapat dibaca kembali dengan syarat menggunakan kunci yang sama untuk proses penyisipan dan pembacaan pesan. Citra hasil penyisipan tidak tahan terhadap operasi penambahan kontras (25%) dan rotasi (90° ke kanan, 90° ke kiri, 180°) serta operasi pemotongan pada sisi atas dan kiri citra, tetapi jika pemotongan pada sisi bawah dan kanan (resolusi citra > 100 piksel) pesan yang disisipkan dapat dibaca kembali dengan benar. Pada citra hasil penyisipan, akan ditemukan *noise* atau titik yang berada pada sisi sebelah kiri atas dari citra karena wilayah tersebut merupakan wilayah awalnya pesan disisipkan.**

Kata kunci*: Steganografi, kriptografi, BPCS, DES, citra *bitmap

ABSTRACT

Bit Plane Complexity Segmentation (BPCS) is steganography method that using uncapability of human's vision in interpreting difficult biner form. Data Encryption Standard (DES) is cryptography algorhytm that is chiper block and changing data become blocks 64 bit and then using encryption key amount 56 bit. By combining steganography algorhytm and cryptography will increase quality of data security. In this research combination of BPCS and DES done by inserting text message into bitmap image, the increating text message restricted maximum 248 characteristic with the long of the key must 16 characteristic in hexsadecimal format. The result obtained by this system testing with image test about 30 images is the inserting text can be read again with the provision of using the same key for inserting process and reading text. This image of insertion result can't stand to adding contrast operation (25%) and rotation (90 to the right, 90 to the left, 180) and cutting operation on the upper side dan left image, but if cutting on the lower side and right (image resolution > 100 piksel) the inserting text can be read again correctly. In image inserting result, will be found noise of the upper left side from image because these region is the initial region is inserted.

Keyword: Steganography, cryptography, BPCS, DES, bitmap image.

I. PENDAHULUAN

Ketika berbagi informasi akan muncul ancaman tentang keamanan informasi atau data yang dibagikan. Oleh karena itu, diperlukan adanya teknik untuk mengamankan informasi atau data seperti kriptografi dan steganografi. *Data Encryption Standard* (DES) merupakan salah satu algoritma kriptografi modern yang diadopsi oleh NIST (*National Institue Of Standards and*

Technology) sebagai standar pengolahan informasi Federal Amerika Serikat. DES mengenkripsikan 64 bit *plaintext* menjadi 64 bit *ciphertext* dengan menggunakan 56 bit *internal key* [6]. *Bit Plane Complexity Segmentation* (BPCS) merupakan teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998. Metode BPCS memanfaatkan perhitungan kompleksitas pada tiap *bit-plane* dalam menyelipkan informasi rahasia [5]. Metode BPCS memanfaatkan perhitungan kompleksitas pada tiap *bit-plane* dalam menyelipkan informasi rahasia. Informasi yang disisipkan seperti teks, gambar, video ataupun audio.

Kriptografi melakukan teknik pengamanan data dengan mengacak informasi sehingga menjadi samar dan sulit dipahami maknanya, sedangkan steganografi ialah teknik menyembunyikan informasi ke dalam media lain sedemikian sehingga seolah-olah menyatu dengan media tersebut. Dengan demikian, kriptografi berfokus pada bagaimana melindungi isi informasi agar tetap aman dan steganografi fokus pada bagaimana agar isi informasi tersebut tidak terlihat keberadaannya. Dengan mengkombinasikan algoritma steganografi dan kriptografi akan meningkatkan kualitas keamanan informasi. Penelitan ini mengkombinasikan metode steganografi BPCS dan kriptografi DES untuk penyisipan pesan teks pada citra *bitmap grayscale* 8 bit.

II. MATERI DAN METODE

2.1 Data Penelitian

Data yang digunakan dalam penelitian ini berupa data citra digital berformat *bitmap grayscale* (*.bmp). Jumlah keseluruhan citra yang akan digunakan adalah 30 citra *bitmap,* dimana 30 citra ini dipakai dalam proses penyisipan pesan dan juga untuk pengujian.

2.2 *Bit-plane complexity segmentation* (BPCS)

BPCS merupakan teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia. Sifat penglihatan manusia yang dimanfaatkan yaitu ketidakmampuan manusia menginterpretasi pola biner yang sangat rumit. BPCS diperkenalkan oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998 [5].

BPCS memiliki beberapa langkah diantaranya yaitu: *bit-plane slicing,* kompleksitas pada *bit-plane*, *informative* dan *noise-like region* serta peta konjugasi.

1) *Bit-plane slicing:* digunakan untuk melihat kontribusi atau pengaruh dari tiap bit penyusun citra. Proses *bit-plane slicing* dimulai dengan menyusun bit urutan terendah atau *Least Significant Bit* (LSB) menjadi *plane* "0" dan urutan tertinggi atau *Most Significant Bit* (MSB) akan disusun menjadi plane "7".
2) Kompleksitas pada *bit-plane*: digunakan sebagai parameter untuk menentukan pesan dapat disisipi dalam *bit-plane* tersebut atau tidak.

   Berikut persamaan kompleksitas:

   $$\boldsymbol{\alpha} = \frac{\mathbf{k}}{\mathbf{n}} \text{ dimana } \mathbf{n} = 2x2^m \text{ x } (2^m\text{-}1) \quad \text{.....(1)}$$

   Dimana:

   α = kompleksitas citra
   k = perubahan warna hitam-putih pada *bit-plane*
   n = nilai perubahan maksimal dalam citra persegi
   m = nilai untuk citra persegi, jika citra 4x4 maka m=2, sedangkan jika 8x8 maka m=3 dengan rumus ukuran citra yaitu 2^m
3) *Informative* dan *noise-like region*: nilai kompleksitas sebuah *bit-plane* digunakan sebagai penentu sebuah bit-plane tergolong *informative* (tidak dapat disisipi pesan) atau *noise-like region* (dapat disisipi pesan). Nilai kompleksitas yang biasa digunakan untuk metode BPCS adalah 0,3. Jika nilai kompleksitas sebuah *bit-plane* dibawah 0,3 maka *bit-plane* tersebut

tergolong sebagai *area informative*, sedangkan jika nilai kompleksitas *bit-plane* diatas 0,3 maka *bit-plane* tersebut tergolong sebagai *noise-like region* [5].

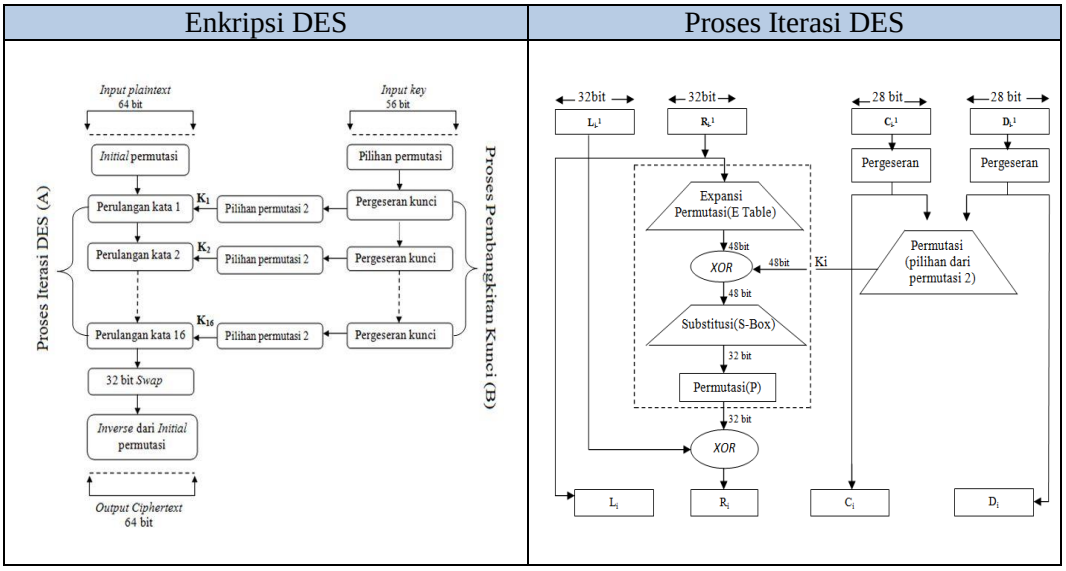
4) Peta konjugasi: digunakan sebagai penanda bahwa sebuah *bit-plane* disisipkan pesan. Peta konjugasi dibuat dalam bentuk satuan bit yang disisipkan pada awalan sebuah *bit-plane* yang disisipi pesan. Baris pertama *bit-plane* yang disisipkan pesan akan diisi dengan nilai bit 1 atau 0. Jika *bit-plane* tersebut merupakan daerah kompleksitas, maka 8 bit awal dari *bit-plane* tersebut akan mengalami sedikit perubahan yaitu 1 bit awal akan digantikan dengan nilai bit "1", sedangkan 7 bit selanjutnya merupakan nilai bit sesuai *bit-plane* yang ada. Selanjutnya sisa bit dari *bit-plane* tersebut akan digantikan dengan biner pesan yang mau disisipkan.

2.3 *Data encryption standard* (DES)

DES termasuk dalam algoritma yang sifatnya *cipher block*, yang berarti DES mengubah data masukkan menjadi blok-blok 64 bit dan kemudian menggunakan kunci enkripsi sebesar 56 bit. Setelah mengalami proses enkripsi maka akan menghasilkan *output* blok 64 bit [2].

1. Algoritma enkripsi DES dan iterasi DES

Algoritma enkripsi dan iterasi DES, ditunjukkan pada gambar 1.



Gambar 1. Algoritma enkripsi dan iterasi DES

Pengolahan menyeluruh pada masing-masing iterasi dapat diikhtiarkan dalam rumus :

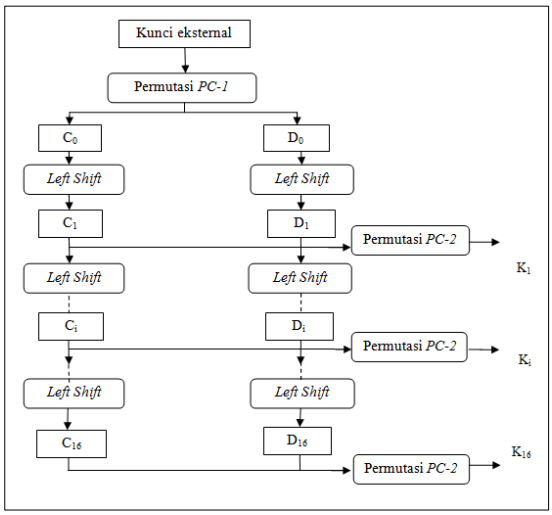
$$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad \text{.....(2)}$$

Dimana :
- L_i = *output* dari sebelah kiri (*left*)
- L_{i-1} = *input* sebelah kiri (*left*)
- R_i = *output* dari sebelah kanan (*right*)
- R_{i-1} = *input* sebelah kanan (*right*)
- $\oplus$ = operasi *XOR*
- f = fungsi permutasi

2. Pembangkitan kunci *internal*

Proses pembangkitan kunci *internal* algoritma DES, ditunjukkan pada gambar 2. [6].

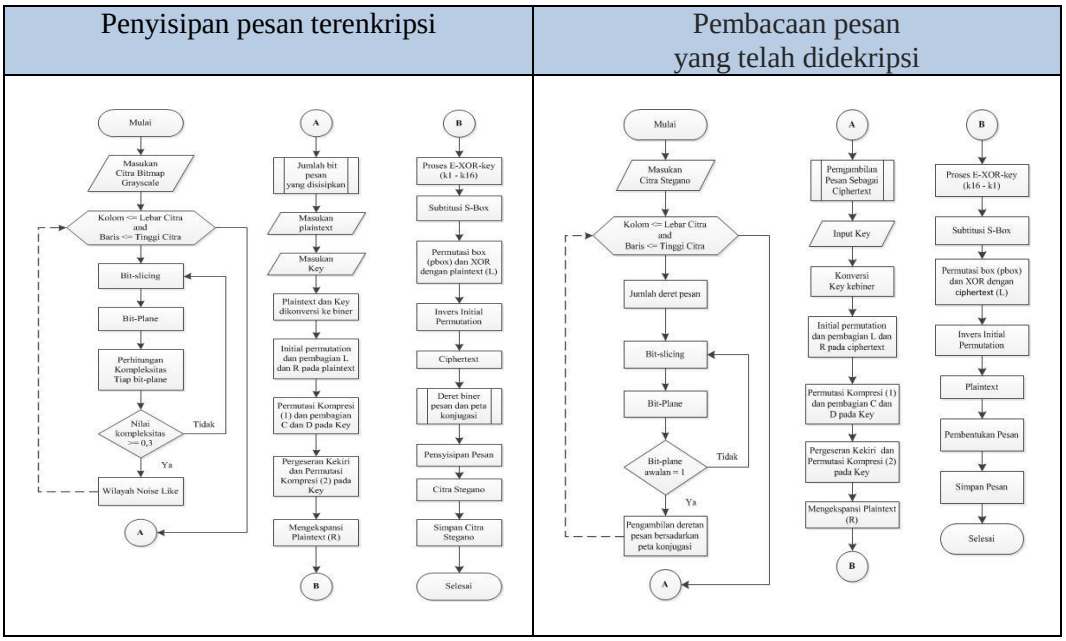
ISSN 2337-7631



Gambar 2. Pembangkitan kunci *internal*

2.4 Arsitektur Sistem

Sistem ini memiliki dua proses utama yaitu proses penyisipan pesan terenkripsi dan pembacaan pesan yang telah didekripsi. Secara garis besar dapat dilihat pada *flowchart* pada gambar 3.



Gambar 3. *Flowchart* penyisipan dan pembacaan pesan

III. HASIL DAN PEMBAHASAN

3.1 Pengujian

Kriteria steganografi yang diuji yaitu:

1. *Fidelity* dan *recovery*: diuji dengan melakukan proses penyisipan pesan teks pada citra. Proses penyisipan pesan ini dilakukan dengan memperhatikan beberapa hal yaitu resolusi citra yang digunakan dan banyaknya pesan yang disisipkan.
   - Citra resolusi 50x50 piksel dengan panjang pesan kurang dari maksimum
   - Citra resolusi 50x50 piksel dengan panjang pesan sama dengan maksimum

- Citra resolusi 50x25 piksel dengan panjang pesan kurang dari maksimum
- Citra resolusi 50x25 piksel dengan panjang pesan sama dengan maksimum
- Citra resolusi lebih besar dari 100 piksel dengan panjang pesan kurang dari maksimum
- Citra resolusi lebih besar dari 100 piksel dengan panjang pesan sama dengan maksimum

2. *Robustness*: diuji dengan melakukan operasi manipulasi terhadap citra hasil. Operasi manipulasi citra yang dilakukan adalah penambahan kontras, rotasi dan pemotongan citra.
   - Operasi penambahan kontras, dilakukan dengan menambah 25% nilai kontras terhadap citra hasil.
   - Operasi rotasi dilakukan dengan merotasi citra hasil 90° ke kanan, rotasi 90° ke kiri dan rotasi 180°.
   - Operasi pemotongan dilakukan dengan memotong sisi atas, kanan, bawah dan kiri dari citra hasil.

3.2 Pembahasan

Berdasarkan hasil pengujian *fidelity* dan *recovery* diperoleh pengaruh hasil resolusi citra terhadap jumlah pesan yang dapat disisipkan, yaitu semakin besar resolusi citra maka jumlah pesan yang dapat disisipkan semakin meningkat, seperti terlihat pada tabel 1.

Tabel 1. Pengaruh resolusi citra terhadap panjang pesan

Resolusi Citra	Panjang Pesan
Kecil (50x50 piksel)	Berkurang
Besar (> 100 piksel)	Bertambah

Selain itu diperoleh hasil bahwa tidak ada pengaruh jumlah pesan yang disisipkan dengan perubahan ukuran citra, yaitu jika pesan yang disisipkan kurang dari atau sama dengan batas maksimum perubahan ukuran citra tetap, seperti terlihat pada tabel 2.

Tabel 2. Pengaruh panjang pesan dengan ukuran citra

Panjang Pesan	Ukuran Citra
Kurang Dari Maksimum (< 248 karakter)	Perubahan Tetap
Sama Dengan Maksimum (= 248 Karakter)	Perubahan Tetap

Dari hasil pengujian penyisipan pesan pada citra, terlihat adanya *noise* atau titik pada citra hasil penyisipan. Hal ini terlihat pada citra berukuran kecil dan memiliki warna yang tidak terlalu kompleks. Berdasarkan hasil pengujian *robustness* menunjukan bahwa operasi manipulasi citra seperti penambahan kontras dan rotasi mempengaruhi proses pembacaan pesan, seperti terlihat pada tabel 3. Hal ini juga ditunjukan pada operasi pemotongan citra, seperti terlihat pada tabel 4.

Tabel 3. Hasil operasi penambahan kontras dan rotasi pada citra hasil

Operasi	+ Kontras 25%	Rotasi 90° ke Kanan	Rotasi 90° ke Kiri	Rotasi 180°
Hasil	Gagal	Gagal	Gagal	Gagal

Tabel 4. Hasil operasi pemotongan pada citra hasil

Resolusi Citra	Hasil Operasi Pemotongan			
	Sisi Atas	Sisi Kanan	Sisi Bawah	Sisi Kiri
Kecil (50x50 Piksel)	Gagal	Gagal	Sukses	Gagal
Besar (> 100 Piksel)	Gagal	Sukses	Sukses	Gagal

ISSN 2337-7631

Dari pengujian *robustness* menunjukan bahwa pembacaan pesan dapat dilakukan apabila wilayah pada citra yang disisipkan pesan tidak mengalami perubahan, wilayah penyisipan pesan yang dimaksud adalah wilayah sebelah kiri atas dari citra dan juga kombinasi pengunaan kuncinya harus sama saat proses penyisipan dan pembacaan pesan.

IV. PENUTUP

4.1 Kesimpulan

Berdasarkan hasil pengujian yang dilakukan pada sistem, disimpulkan beberapa hal sebagai berikut:

1. Proses penyisipan pesan pada citra untuk penerapan kombinasi steganografi *Bit Plane Complexity Segmentation* (BPCS) dan kriptografi *Data Encryption Standard* (DES) menggunakan 30 citra *bitmap* dengan rincian 10 citra *bitmap* simetri resolusi 50 x 50 piksel, 10 citra *bitmap* asimetri resolusi 50 x 25 piksel, dan 10 citra *bitmap* asimetri resolusi diatas 100 piksel dapat berjalan dengan baik, pesan yang disisipkan dapat dibaca kembali dengan syarat menggunakan kunci yang sama untuk proses penyisipan dan pembacaan pesan. Kombinasi yang dihasilkan dapat digunakan untuk peningkatan keamanan data.
2. Panjang pesan teks yang disisipkan pada citra bergantung pada resolusi citra. Semakin besar resolusi citra, maka jumlah pesan yang disisipkan semakin bertambah.
3. Pada citra hasil penyisipan, akan ditemukan *noise* atau titik yang berada pada sisi sebelah kiri atas dari citra karena wilayah tersebut merupakan wilayah awalnya pesan disisipkan.
4. Citra hasil penyisipan tidak tahan terhadap operasi penambahan kontras (25%) dan rotasi (90° ke kanan, 90° ke kiri, 180°) serta operasi pemotongan pada sisi atas dan kiri citra, tetapi jika pemotongan pada sisi bawah dan kanan (resolusi citra > 100 piksel) pesan yang disisipkan dapat dibaca kembali dengan benar, dengan syarat menggunakan kunci yang sama untuk proses penyisipan dan pembacaan pesan.

4.2 Saran

Berdasarkan pembahasan sebelumnya, maka saran untuk pengembangan selanjutnya adalah:

a. Media penampung yang digunakan bukan saja media citra tetapi juga media lain seperti media *audio* atau media *video*.
b. Jumlah pesan yang disisipkan dapat lebih besar dari 248 karakter.

DAFTAR PUSTAKA

[1] Anandita, E. R., 2014, *Klasifikasi Tebu dengan Menggunakan Algoritma Naïve Bayes Classification pada Dinas Kehutanan dan Perkebunan Pati*, Universitas Dian Nuswantoro, Semarang.

[1] Angraini dan Uma,U., 2007, *Analisis Penyisipan Data Pada Citra Bitmap Menggunakan Metode Bit Plane Complexity Segmentation*, STMIK Amikom, Yogyakarta.

[2] Ariyus, D., 2006, *Kriptografi Keamanan Data dan Komunikasi*, Graha Ilmu, Yogyakarta.

[3] Firmansyah R., 2011, *Implementasi Kriptografi dan Steganografi pada Media Gambar dengan Menggunakan Metode DES dan Region-Embed Data Density*, Institut Teknologi Sepuluh Nopember, Surabaya.

[4] Irawan P. L. T., 2014, *Implementasi Kripto - Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital*, STIKI, Malang.

[5] Kawaguchi, E., dan Eason, R.E.,1998, *Principle and applications of BPCS-steganography*, Kyushu Institude of Technology, Japan.

[6] Munir, R., 2006, *Kriptografi*, Informatika, Bandung.

[7] Obije S. Y., 2016, *Implementasi Steganografi Menggunakan Metode Bit Plane Complexity Segmentation (BPCS) pada Citra Bitmap Grayscale 8 Bit*, Universitas Nusa Cendana, Kupang.

[8] Perkhasa Y. B., 2012, *Implementasi Kriptografi dan Steganografi pada File Audio Menggunakan Metode DES dan Parity Coding*, Institut Teknologi Sepuluh Nopember, Surabaya.

[9] Prasetiyo B., 2014, *Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data*, Universitas Negeri Semarang, Semarang.

[10] Sadikin, R., 2012, *Kriptografi Untuk Keamanan Jaringan*, ANDI,Yogyakarta.