p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

DESAIN ALGORITMA STEGANOGRAFI DENGAN METODE *SPREAD SPECTRUM* BERBASIS PCMK (PERMUTASI *CHAOTIC* MULTIPUTARAN MENGECIL DAN MEMBESAR) YANG TAHAN TERHADAP GANGGUAN

Septian Rheno Widianto
Prodi Teknologi Rekayasa Perangkat Lunak Politeknik Enjinering Indorama Kembang Kuning Ubrug Jatiluhur, Purwakarta
septian.rheno@pei.ac.id

Abstrak

Kriptografi dan steganografi adalah dua alat untuk menawarkan keamanan data. Kriptografi menyediakan fitur seperti kerahasiaan, keaslian, dan integritas data. Pada steganografi ada 3 hal penting yang perlu diperhatikan yaitu *imperceptibility*, *fidelity*, dan *recovery*, Steganografi biasanya terdiri dari dua sistem, yaitu sistem untuk menyembunyikan pesan dan sistem untuk mengambil pesan. Metode steganografi yang dipakai merupakan metode yang berbasis sistem *chaos*, dalam ilmu fisika dan matematika, teori *chaos* berhubungan dengan suatu kegiatan atau kebiasaan sistem *non-linear* yang dinamis, yang untuk beberapa kondisi menampilkan sebuah fenomena acak (*chaos*). *Spread Spectrum steganography* terpencar-pencar sebagai pesan yang diacak (*encrypt*) melalui gambar. Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode permutasi multiputaran memiliki dua pasang metode yaitu permutasi multiputaran mengecil (PCMPK) dan permutasi multiputaran membesar (PCMPB) yang merupakan proses kebalikan satu dengan lainnya. Metode yang diusulkan juga diukur kinerjanya dari sisi ketahanan terhadap gangguan, diantaranya terhadap kompresi JPEG, terhadap gangguan standar (*Gaussian noise*, *Poisson noise*, *Salt and Pepper noise*, dan *speckle noise*), terhadap kehilangan data, serta terhadap perubahan kecerahan dan kontras. Dari beberapa hasil analisis dapat disimpulkan kinerja algoritma steganografi yang dihasilkan dapat tahan tehadap gangguan gangguan terhadap kompresi JPEG, terhadap *noise* standar (*Gaussian noise*, Poisson *noise*, *Salt and Pepper noise*, dan *speckle noise*), terhadap kehilangan data, serta terhadap perubahan kecerahan dan kontras

Kata kunci: Kriptografi, Steganografi, Chaos, PCMK/B, Spread Spectrum

PENDAHULUAN

Kemajuan teknologi Internet, media digital seperti gambar, audio, video dan teks dibagi dan dikirimkan melalui Internet dengan lebih mudah. Namun, salah satu tantangan utama dalam berbagi dan mentransmisikan semua jenis informasi melalui saluran publik adalah keamanan data. Oleh karena itu, beberapa cara untuk melindungi informasi yang dikirimkan terhadap seorang penyadap dan pihak yang tidak berwenang menjadi sebuah kebutuhan.

Kriptografi dan steganografi adalah dua alat untuk menawarkan keamanan data. Kriptografi menyediakan fitur seperti kerahasiaan, keaslian, dan integritas data. Misalnya, kerahasiaan data dihasilkan melalui algoritma enkripsi yang mengacak / mencampur informasi pribadi sehingga menjadi tidak dapat dibaca oleh pihak selain penerima yang dimaksud. Secara khusus, dalam aplikasi kriptografi, pihak penyadap / pihak yang tidak berwenang mengetahui adanya informasi pribadi, dan tantangannya adalah menguraikan informasi yang dienkripsi. Di sisi lain, steganografi memberikan keamanan data dengan menyembunyikan informasi sehingga keberadaan pesan tersembunyi tidak diketahui oleh penyusup.

Citra digital digunakan sebagai pembawa informasi tersembunyi karena tingginya tingkat redundansi di dalamnya yang disebabkan oleh

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

rendahnya sensitivitas sistem visual manusia, pesan tersembunyi mungkin dari jenis apa pun seperti teks, gambar, audio, atau video. Tantangan utama dalam aplikasi steganografi adalah bahwa pesan tersebut harus disembunyikan didalam gambar sedemikian rupa sehingga *stego-image* yang dihasilkan tidak menyimpang jauh dari citra aslinya, secara visual dan statistik.

Pada steganografi ada 3 hal penting yang perlu diperhatikan yaitu (1) *imperceptibility*, adalah keberadaan pesan tidak dapat dipersepsi oleh indrawi manusia, (2) *fidelity*, adalah mutu dari media steganografi tidak mengalami perubahan signifikan akibat proses penyisipan, dan (3). *recovery*, adalah pesan dapat diekstraksi sewaktu-waktu saat dibutuhkan [Munir, R. 2004].

Steganografi biasanya terdiri dari dua sistem, yaitu sistem untuk menyembunyikan pesan dan sistem untuk mengambil pesan. Dalam sistem-sistem tersebut terkandung enam komponen penyusun, antara lain [Lin, Eugene T. and Delp, Edward J. 2004]: (1) Pesan Rahasia, (2) Cover Document,

(3) Stego Document, (4) Stego Key, (5) Fungsi Penyembunyi $f'(M,C,K) \rightarrow Z$, (6) Fungsi Detektor $f'(Z,C,K) \rightarrow M$.

Steganografi dapat diterapkan pada hampir semua jenis file multimedia, tetapi yang paling sering digunakan adalah pada citra digital, karena pertukaran data dalam bentuk citra digital pada jaringan internet saat ini cukup tinggi, sehingga dapat mengurangi kecurigaan akan adanya pesan rahasia yang telah disisipkan. *Cover document* dari komponen-komponen penyusun steganografi yang terdapat di steganografi gambar digital adalah sebuah citra digital atau biasa disebut *cover-image*.

Steganogafi ini akan menghasilkan *output* berupa citra baru yang mengandung pesan yang sudah disembunyikan oleh algoritma steganografi, secara umum disebut *stego-image*. Dalam steganografi pengirim dan penerima harus memiliki kunci *(stego-key)* yang sama yang tentunya dirahasiakan dari pihak-pihak lain yang tak diinginkan untuk mengetahui isi pesan tersebut. Selain itu penerima harus menggunakan gambar yang mengandung pesan tersembunyi *(stego-image)* untuk dapat menerima pesan rahasia tersebut.

Metode steganografi yang dipakai merupakan metode yang berbasis sistem *chaos*, dalam ilmu fisika dan matematika, teori *chaos* berhubungan dengan suatu kegiatan atau kebiasaan sistem *non-linear* yang dinamis, yang untuk beberapa kondisi menampilkan sebuah fenomena acak (*chaos*) [Wikipedia. Chaotic. 2017]. *Chaotic* merupakan suatu sistem yang dinamis yang mempunyai prilaku terbatas.

Dua karakteristik yang dimiliki sinyal *Chaotic* adalah *spectrum* daya yang kontinus pada suatu pita frekuensi tertentu, dari ciri ini menunjukan bahwa sinyal *Chaotic* merupakan sinyal yang nonlinier sekaligus sering dikatakan sinyal *noise*, dan mempunyai kepekaan yang tinggi terhadap kondisi awal [Supangat, Suhono H., Juanda, Kuspriyanto. 2000]. Pada aplikasinya sinyal *Chaotic* dapat berfungsi sebagai algoritma pemetaan dan sebagai pembangkit kode-kode *random* yang tidak mempunyai pola.

Spread spectrum dalam dunia komunikasi merupakan proses sinyal pita sempit dimodulasi oleh sinyal pita lebar yang akan menyebar sinyal pita sempit tersebut [Marloe, Hamidah. 2003]. Dalam *steganography*, sinyal pita sempit dianalogikan dengan *hidden data* yang akan disisipkan dan sinyal pita lebar dianalogikan sebagai citra digital yang telah didekomposisi *wavelet* atau media digital yang akan disisipi *hidden data*.

Dalam penelitian ini, diajukan sebuah algoritma steganografi baru permutasi *Chaotic* berbasis multiputaran mengecil dan membesar (PCMPK/B) yang memiliki ruang kunci yang sangat besar, sehingga dapat diterapkan untuk metode steganografi yang tahan terhadap *brute force attack* serta dapat mengantisipasi kebutuhan ruang kunci yang besar.

Metode tersebut dikembangkan dalam perangkat lunak berbasis C#, dan diimplementasikan dalam perangkat lunak Matlab untuk steganografi citra digital dengan tingkat keamanan tinggi, proses yang cepat, dan sekaligus tahan terhadap gangguan yang dapat digunakan untuk mengantisipasi perkembangan pertukaran informasi melalui sosial media, M2M, dan IOT. Metode PCMPK/B juga diimplementasikan dalam algoritma enkripsi *Chaotic Encryption System* (CES) yang dikembangkan dalam perangkat lunak berbasis C.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

PEMBAHASAN

Beberapa hal yang menjadi perhatian dalam pembahasan, yaitu :

a. Steganografi.
b. Sistem *Chaos* (*Chaos*).
c. Spread Spectrum.
d. Analisis Stegano Citra.
e. Algoritma Permutasi *Chaotic* Multiputaran Membesar (PCMB).
f. Algoritma Permutasi *Chaotic* Multiputaran Mengecil (PCMPK).

Steganografi

Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. [C. Cachin. 2005] Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Oleh karena itu, berbeda dengan kriptografi, dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui adanya pesan rahasia. Pesan rahasia tidak diubah menjadi karakter 'aneh' seperti halnya kriptografi.
Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau media digital lainnya dan terlihat seperti pesan biasa.

Dalam steganografi dikenal beberapa terminology, *cover-data* atau *cover-text* merupakan media penyembunyi pesan. Sedangkan hasil penggabungan antara *cover-data* dengan pesan yang disembunyikan disebut *stego-text, stego-data,* atau *stego-object.* Algoritma yang menghasilkan *stego text* disebut *stegosystem*. Pihak yang menciptakan *stegosystem* disebut steganografer. [C. Cachin. 2005].

Secara umum *stegosystem* terdiri dari tiga tahap yaitu algoritma untuk mendapatkan kunci, mengkodekan pesan, dan men-*decode* pesan. Algoritma tersebut dibungkus dalam suatu teknik tehnik penyembunyian pesan yang bermacam-macam [C. Cachin. 2005].


Gambar 2.1 Cover-data dan 2.2 Stego-data.

Gambar 2.1 merupakan *file* gambar lena.jpg yang dijadikan sebagai *cover data*. Sedangkan gambar 2.2 merupakan *file* gambar lena.jpg yang telah dimasukan pesan rahasia berupa teks melalui aplikasi steganografi. Terlihat bahwa dengan mata manusia yang terbatas, perbedaan kedua gambar tersebut tidak terlihat. Keberadaan pesan rahasia di dalam gambar 2.2 pun tidak dapat diketahui keberadaannya oleh pihak lain [R. Mutia S. 2017].

Sistem *Chaos* (*Chaos*)

Sistem *chaos* adalah sistem deterministik yang acak, namun definisi sistem *chaos* adalah *tricky* dan para ahli tidak menemukan kata yang sepakat untuk definisi *chaos* seperti disampaikan oleh Weisstein [E. W. Weisstein. 2015]. Hal ini juga sejalan dengan yang disampaikan oleh Gleick [J. Gleick. 1997] bahwa tidak ada ahli sistem *chaos* yang diwawancarainya setuju dengan definisi dari kata *chaos* itu sendiri.

Perbedaan mengenai definisi *chaos* juga terdapat dalam beberapa buku yang menjadi referensi mengenai *chaos*, seperti Wiggins [S. Wiggins. 2003] berpendapat bahwa sebuah sistem dinamis yang menunjukkan sensitivitas terhadap nilai kondisi awal dalam *set invariant* yang tertutup dengan lebih dari satu orbit dapat disebut sebagai sistem *chaos*. Sementara itu Tabor [M. Tabor. 1989] berpendapat bahwa solusi *Chaotic* adalah solusi deterministik yang memiliki hasil yang sensitif terhadap kondisi awal dan dalam *phase space* nampak sangat random.

Berikut ini akan dijelaskan sekilas tentang teori *Chaos* yang sebagian besar merujuk dari pendapat Kocarev dan Lian dalam bukunya *Chaos-Based Cryptography* [L. Kocarev and S. Lian. 2011] seperti dijabarkan dalam bagian studi pustaka oleh Suryadi [M. Suryadi. 2013]. Teori *Chaos* merupakan sebuah

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

teori yang pada awalnya berkembang dalam bidang fisika.

Dalam pandangan teori *chaos* bahwa alam semesta yang tampak teratur atau terprediksi, ternyata tidaklah demikian. Hal tersebut diungkapkan oleh Edward Lorenz [E. N. Lorenz. 1995], yang pertama kali menemukan dan memperkenalkan fenomena *chaos* yang disebut dengan istilah "efek kupu-kupu".

Chaos, menurut Ian Stewart [I. Stewart. 2000] adalah perubahan yang sangat kompleks, *iregular* dan acak di dalam sebuah sistem yang deterministik. *Chaos* adalah suatu keadaan di mana sebuah sistem tidak dapat diprediksi akan ditemukan di tempat berikutnya. Sistem ini bergerak secara acak. Namun, bila keadaan acak tersebut diperhatikan dalam waktu yang cukup lama dengan mempertimbangkan dimensi waktu, maka akan ditemukan juga keteraturan. Karena bagaimanapun kacaunya sebuah sistem, maka sistem tidak akan pernah melewati batas-batas tertentu. Bagaimanapun acaknya sebuah sistem, ruang geraknya tetap dibatasi oleh sebuah kekuatan penarik yang disebut *strange attractor*. *Strange attractor* di satu sisi menjadikan sebuah sistem bergerak secara acak, dinamis, dan fluktuatif. Di sisi lain akan membingkai batas-batas ruang gerak tersebut.

Spread Spectrum

Metode *spread spectrum* dalam steganografi diilhamidari skema komunikasi *spread spectrum*, yang mentransmisikan sebuah sinyal pita sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi. *Spread Spectrum steganography* terpencar-pencar sebagai pesan yang diacak (*encrypt*) melalui gambar. Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image* (gambar) [P. Budi. 2011].

Pada proses penyembunyian data, bit-bit informasi yang telah mengalami proses *spreading* ini kemudian akan dimodulasi dengan *pseudo-noise signal* yang dibangkitkan secara acak berdasarkan kunci penyembunyian. Hasil dari proses modulasi ini kemudian digabungkan sebagai *noise* ke dalam sebuah berkas media pada bit-bit terakhir dari berkas media. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise signal* tersinkronisasi. Media yang telah berisi informasi rahasia tersebut disaring terlebih dahulu dengan proses *pre-filtering* untuk mendapatkan *noise. Noise* yang dihasilkan selanjutnya dimodulasi dengan menggunakan *pseudo-noise signal* untuk mendapatkan bit-bit yang berkorelasi. Bit-bit yang berkorelasi tersebut dianalisa dengan perhitungan tertentu untuk menghasilkan bit-bit informasi yang sesungguhnya [P. Budi. 2011].

Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan metode *spread spectrum* memperlakukan *cover-object* sebagai derau (*noise*) ataupun sebagai usaha untuk menambahkan derau semu (*pseudo-noise*) ke dalam *cover-object*. *Cover-object* sebagai derau Sistem yang memperlakukan *cover-object* sebagai derau dapat menambahkan sebuah nilai ke dalam *cover-object*. Nilai ini harus ditransmisikan di bawah tingkat derau yang ditambahkan nilai ke dalamnya. Hal ini berarti kapasitas sangat ditentukan oleh *cover-object*.

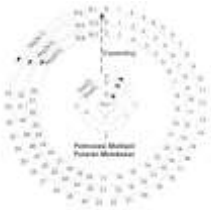
Analisis Stegano Citra

Analisis stegano citra yang dilakukan untuk mengukur hasil kinerja metode stegano citra adalah: visualisasi, analisis statistik (*histogram*, korelasi, entropi, analisis kerandoman NIST), analisis diferensial (NPCR, UACI), analisis sensitivitas terhadap kunci (NPCR, UACI, korelasi), dan ruang kunci. Metode yang diusulkan juga diukur kinerjanya dari sisi ketahanan terhadap gangguan, diantaranya terhadap kompresi JPEG, terhadap gangguan standar (*Gaussian noise, Poisson noise, Salt and Pepper noise,* dan *speckle noise*), terhadap kehilangan data, serta terhadap perubahan kecerahan dan kontras.

Algoritma Permutasi Chaotic Multiputaran Membesar (PCMB)

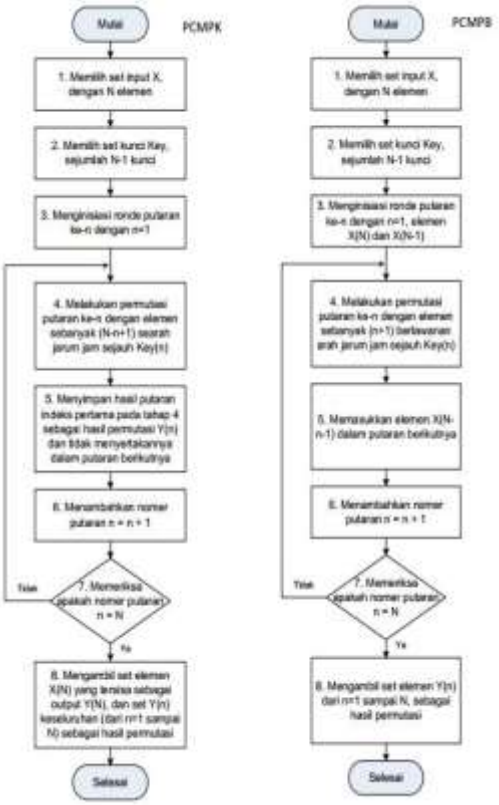
Untuk mendapatkan *set* elemen asli dari elemen yang diacak menggunakan metode PCMPK adalah dengan melakukan permutasi multiputaran membesar (PCMPB) yang dikontrol oleh rangkaian kunci *Key* yang sama. Berkebalikan dengan PCMPK, jumlah elemen yang terlibat dalam setiap ronde putaran pada PCMPB semakin berkembang yang secara visual. [Y. Suryanto. 2016]. digambarkan dalam Gambar 2.3. Algoritma PCMPB dijabarkan sebagai berikut:

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 2.3 Visualisasi Permutasi Chaotic Multiputaran Membesar (PCMPB) untuk Elemen [Y. Suryanto. 2016]

Algoritma PCMPK dan PCMPB digambarkan dalam Gambar 2.4 berikut:



Gambar 2.4 Algoritma permutasi Chaotic multiputaran mengecil (PCMPK) dan membesar (PCMPB) [Y. Suryanto. 2016]

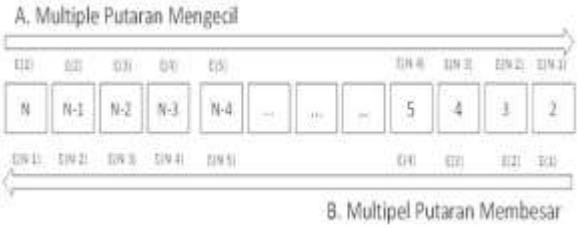
1. Memilih *set* input *X*, dengan *N* elemen.
2. Memilih set kunci *Key* sejumlah $N - 1$ rangkaian kunci *Key*(*n*). (*Key*(*n*) dapat dipilih sembarang angka bilangan bulat dalam ruang kunci sesuai dengan Gambar 3.3.
3. Menginisiasi ronde putaran ke-*n* dengan $n = 1$, dua elemen terakhir $X(n)$ dan $X(n-1)$.
4. Melakukan permutasi putaran ke-n dengan elemen sebanyak $(n + 1)$ searah jarum jam sejauh *Key*(*n*).
5. Memasukkan elemen $X(N - n - 1)$ pada elemen hasil putaran tahap 4 sebagai tambahan elemen input dalam putaran berikutnya.
6. Menambahkan nomer putaran $n = n + 1$.
7. Memeriksa apakah nomer putaran $n = N$, jika tidak ulangi langkah 4 dan jika iya lanjutkan ke langkah 8.
8. Mengambil *set* elemen $Y(n)$ dari $n = 1$ sampai sebagai hasil permutasi PCMPB.

Algoritma Permutasi Chaotic Multiputaran Mengecil (PCMK)

Metode permutasi multiputaran memiliki dua pasang metode yaitu permutasi multiputaran mengecil (PCMPK) dan permutasi multiputaran membesar (PCMPB) yang merupakan proses kebalikan satu dengan lainnya. Visualisasi permutasi PCMPK [Y. Suryanto. 2016].

Algoritma PCMPK dijabarkan sebagai berikut:

1. Memilih set input X , dengan elemen.
2. Memilih set kunci Key sejumlah $N - 1$ rangkaian kunci *Key*(*n*). *Key*(*n*) dapat dipilih sembarang angka bilangan bulat positif dalam ruang kunci sesuai dengan Gambar 2.5.



Gambar 2.5 Ruang kunci untuk tiap tahap putaran permutasi multiputaran. [Y. Suryanto. 2016].

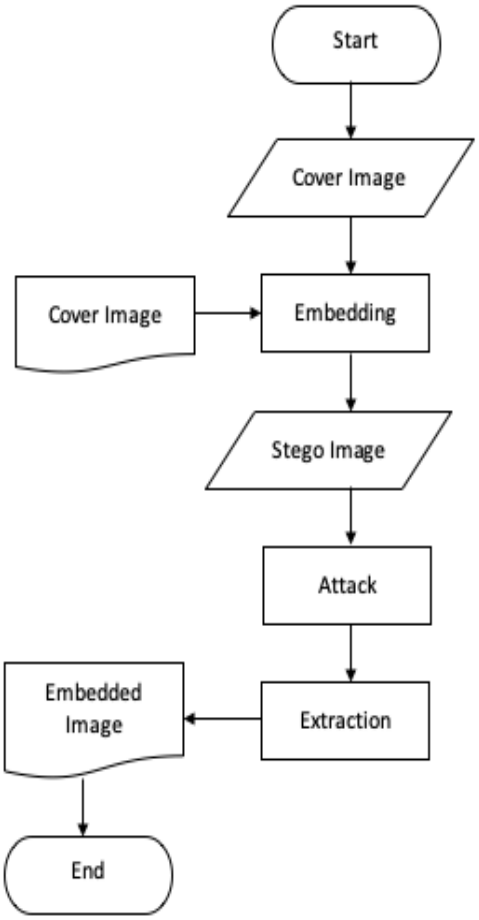
3. Menginisiasi ronde putaran ke-*n* dengan $n = 1$.
4. Melakukan permutasi putaran ke-*n* dengan elemen sebanyak $(N - n + 1)$ searah jarum jam sejauh *Key* (*n*).
5. Menyimpan hasil putaran indeks pertama (Y_n) pada tahap 4 sebagai hasil permutasi putaran pertama dan tidak menyertakannya dalam putaran berikutnya.
6. Menambahkan nomer putaran $n = n + 1$.
7. Memeriksa apakah nomer putaran $n = N$, jika tidak ulangi langkah 4, dan jika iya lanjutkan ke langkah 8.
8. Mengambil *set* elemen X (*n*) yang tersisa sebagai output $Y(n)$ yang terakhir, dan *set* $Y(n)$ dari $n = 1$ sampai N sebagai hasil permutasi PCMPK.

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

METODOLOGI PENELITIAN

Perancangan Sistem

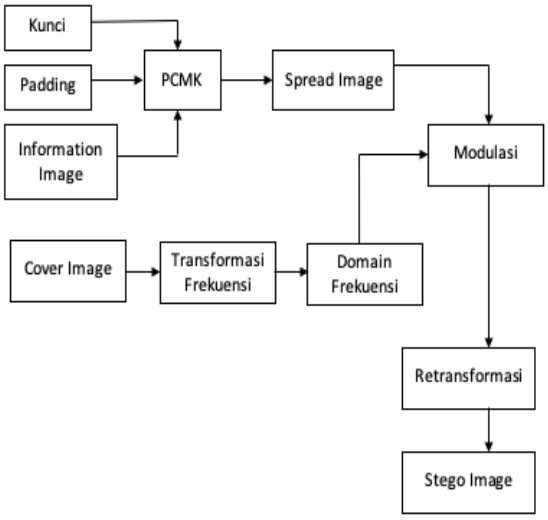
Blok diagram steganografi pada citra digital adalah sebagai berikut



Gambar 3.1 Diagram Alir Sistem.

Penyisipan Pesan

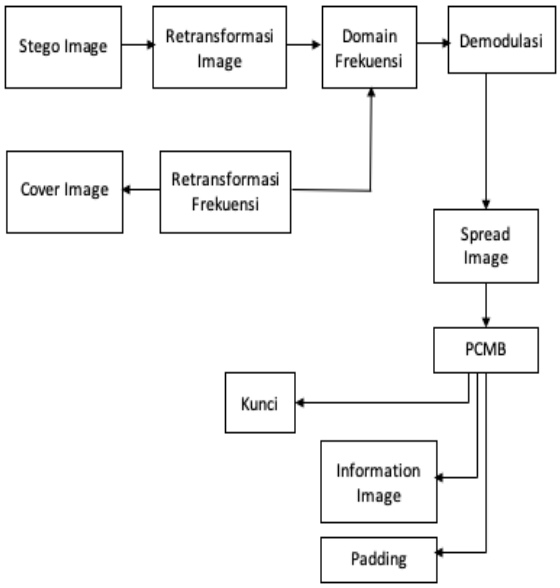
Diagram Blok penyisipan pesan pada citra digital adalah sebagai berikut:



Gambar 3.2 Diagram Blok Penyisipan Pesan.

Ekstrasi Pesan

Diagram Blok ekstrasi pesan pada citra digital adalah sebagai berikut:



Gambar 3.3 Diagram Blok Ekstrasi Pesan.

PEMBAHASAN

Bertujuan untuk menghasilkan aplikasi steganografi berbasis Permutasi *Chaotic* Multiputaran Membesar dan Mengecil (PCMK/B) yang dibuat dengan menggunakan *software* Matlab_R2016b.

Algoritma steganografi berbasis PCMK/B yang dihasilkan merupakan algoritma steganografi yang tahan terhadap gangguan, gangguan yang dimaksud meliputi gangguan terhadap kompresi JPEG, terhadap *noise* standar (*Gaussian noise*, Poisson *noise*, *Salt and Pepper noise*, dan *speckle noise*), terhadap kehilangan data, serta terhadap perubahan kecerahan dan kontras.

Pseudocode PCMK

Percobaan permutasi *chaotic* multiputaran mengecil (PCMK) dilakukan pada *software* Matlab_R2016b, berikut ini adalah *pseudocode* dari PCMK

```
function Y = ACPMCSM2(X,keys);
%function CPMCSM, chaotic permutation multicircular shrinking movement
%Mencari ukuran dari element yang akan dipermutasi
NSize = length(X);
kunci = keys;
```

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

```
%ACPMCSM permutation
%Y = uint8(zeros(1,NSize));
index = 0;
for n=1:(NSize-1)
  index =mod(index+(kunci(n)),NSize-
  n+1);
  Y(n) = X(index+1); %Melakukan
permutasi untuk urutan index, dilakukan
penyesuaian index karena matlab dari 1
  X(index+1) = []; %Data yang sudah
terpakai tidak disertakan lagi
end
Y(NSize) = X(1);
```

Pseudocode PCMB

Percobaan permutasi *chaotic* multiputaran membesar (PCMB) dilakukan pada *software* Matlab_R2016b, berikut ini adalah *pseudocode* dari PCMB

```
function Y = CPMCEM2(X, keys);
%function CPMCEM2, chaotic
permutation multicircular expanding
movement
%mempercepat proses CPMCEM
%Untuk jumlah elemen besar bisa
mempercepat, seperti N=100000; CPMCEM
136,55
%detik sedangkan CPMCEM2 bisa
26,66 detik. Untuk elemen kecil hampir
sama
%Keluaran uint8 untuk image
%Mencari ukuran dari element yang
akan dipermutasi
NSize      = length(X);
for n=1:NSize-1
  Y = X(NSize-n:NSize);
  index = mod(-keys(NSize-n),n+1)+1;
  X(NSize-n:NSize+1-index) =
  Y(index:n+1);
  if index > 1
    X(NSize+2-index:NSize) =
    Y(1:index-1);
  end
 Y = X;
end
end
```

KESIMPULAN

Dari beberapa hasil analisis dapat disimpulkan kinerja algoritma steganografi yang dihasilkan dapat tahan tehadap gangguan gangguan terhadap kompresi JPEG, terhadap *noise* standar (*Gaussian noise*, Poisson *noise*, *Salt and Pepper noise*, dan *speckle noise*), terhadap kehilangan data, serta terhadap perubahan kecerahan dan kontras.

Algoritma steganografi digabungkan dengan metode *spread spectrum* berfungsi untuk menyebar informasi yang terdapat didalam *embedded image* sehingga tidak diketahui keberadaan/posisi dari pesan yang disisipkan tersimpan, sehingga pengirim pesan pun tidak mengetahui posisi dari pesan yang terdapat didalam *embedded image.*

Pada penyisipan pesan menggunakan Permutasi *Chaotic* Multiputaran Mengcil (PCMK) untuk proses yang bersumber dari kunci, *padding*, dan *information image* menghasilkan *spread image* yaitu mengacak informasi yang telah didapatkan dari proses sebelumnya menjadi *spread image*. Proses dari *cover image* diawali dengan melakukan transformasi frekuensi menjadi domain frekuensi, kemudian disatukan dengan hasil dari proses *spread image* untuk dilakukan retransformasi sehingga menghasilkan sebuah *stego image.*

Proses ekstrasi pesan diawali dengan *stego image* yang telah dihasilkan untuk dilakukan retransformasi image kemudian diubah kedalam domain frekuensi dan dilakukan demodulasi, dari proses demodulasi menghasilkan 2 proses yang pertama adalah melakukan retransformasi frekuensi dan menghasilkan sebuah *cover image* dan yang kedua melakukan *spread image* menggunakan permutasi *chaotic* multiputaran membesar (PCMB) yang akan menghasilkan kunci, information image dan padding, meskipun pada hasil akhir padding yang ditambahkan pada proses awal tidak digunakan lagi pada hasil akhir dari proses steganografi citra.

DAFTAR PUSTAKA

[1] C. Cachin (2005) : *Digital Steganography*
[2] E. N. Lorenz, "*The essence of chao"s*: University of Washington Press, 1995.
[3] E. W. Weisstein. (4/16/2015). "*Chaos"*. Available: From MathWorld-A Wolfram Web Resource. *http://mathworld.wolfram.com/Chaos.html.*

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

[4] I. Stewart, "*Mathematics: The Lorenz attractor exists*," *Nature*, vol. 406, pp. 948-949, 2000.
[5] J. Gleick, Chaos: "*Making a new science"*: Random House, 1997.
[6] Lin, Eugene T. and Delp, Edward J. "*A Review of Data Hiding in Digital Image"*, *http://www.ece.purdue.edu/~ace*, 18 Juli 2004.
[7] L. Kocarev and S. Lian, "*Chaos-based cryptography": theory, algorithms and applications* vol. 354: Springer, 2011.
[8] Marloe, Hamidah**, "***Implementasi Autentikasi Citra Digital Menggunakan Watermark Berupa Hash Citra Dengan Transformasi Fourier"*. STT Telkom, Bandung. 2003.
[9] M. Tabor, "*Chaos and Integrability in Nonlinear Dynamics": An Introduction*: Wiley-Interscience, 1989.
[10] M. Suryadi, "*Algoritma Baru Enkripsi Video dengan Menggunakan Multi Chaotic Cipher Berbasis Galois Field (256) dan Transformasi Cosinus Diskrit Terkuantisasi*," Disertasi Doktor, *Department of Electrical Engineering*, Universitas Indonesia, Indonesia, 2013.
[11] Munir, R. (2004) : "*Pengolahan Citra Digital", Informatika*, Bandung.
[12] P. Budi, "*Steganografi Pada Citra Digital Menggunakan Metode Spread Spectrum Dan Metode Least Significant Bit (LSB) Modification*", Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia. 2011.
[13] R. Mutia S "*Studi dan Pengujian Algoritma Steganografi pada Aplikasi Steghide*", Institut Teknologi Bandung, Indonesia. 2017.
[14] S. Wiggins, "*Introduction to applied nonlinear dynamical systems and chaos"* vol. 2: Springer Science & Business Media, 2003.
[15] Supangkat, Suhono H., Juanda, Kuspriyanto. "*Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital"*. ITB, Bandung. 2000.
[16] Y. Suryanto, "*Pengembangan dan analisis metode permutasi Chaotic baru berbasis multiputaran mengecil dan membesar untuk enkripsi citra dengan tingkat keamanan tinggi, cepat dan tahan terhadap gangguan".* Disertasi Program Doktor, Universitas Indonesia. 2016.