Algoritma B217AN menggunakan Metode *Spread Spectrum*Berbasis PCMK/PCMB

Septian Rheno Widianto
Prodi Teknologi Rekayasa Perangkat Lunak
Politeknik Enjinering Indorama
Purwakarta - Indonesia
septian.rheno@pei.ac.id

Spread spectrum dalam dunia komunikasi merupakan proses sinyal pita sempit dimodulasi oleh sinyal pita lebar yang akan menyebar sinyal pita sempit tersebut *Output* atau hasil dari algoritma steganografi yang berupa citra baru mengandung pesan yang sudah disembunyikan *(stego-image)*. Pengirim dan penerima harus memiliki *stego-key* yang sama dan dirahasiakan dari pihak yang tidak diizinkan untuk mengetahui isi pesan tersebut. Penerima harus menggunakan gambar yang berisi *stego-image* untuk dapat menerima pesan rahasia tersebut. Kinerja algoritma steganografi yang dihasilkan dapat tahan perubahan kecerahan dan kontras kompresi JPEG, *Gaussian noise, Poisson noise, Salt and Pepper noise,* dan *speckle noise, data loss*.

Kata Kunci: stego-image,stego-key, Spread Spectrum.

1. PENDAHULUAN

Metode keamanan data yang efektif dilakukan adalah menggunakan penggabungan kriptografi dan steganografi. 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.

Steganografi terdiri dari dua system: (1) sistem agar pesan tersembunyi dan agar pesan dapat diambil. Enam komponen penyusun terdapat didalam system tersebut, yaitu [Lin, Eugene T. and Delp, Edward J. 2004]: (1) Pesan Rahasia (2) Cover Document, (3) Stego Document, (4) Stego Key, (5) Fungsi untuk menyembunyikan $f'(M,C,K) \rightarrow Z$, (6) Fungsi Pendeteksi $f'(Z,C,K) \rightarrow M$.

Penerapan steganografi dapat digunakan di semua file multimedia, dan citra digital merupakan yang paling sering digunakan, dikarenakan dalam bentuk citra digital pertukaran data di sebuah jaringan internet cukup *massive*, dan diharapkan mengurangi factor kecurigaan pesan rahasia yang telah disisipkan. *Cover document* dari komponen-komponen penyusun steganografi yang terdapat di steganografi gambar digital yaitu *cover image* (Citra Digital).

Output atau hasil dari algoritma steganografi yang berupa citra baru mengandung pesan yang sudah disembunyikan *(stego-image)*. Pengirim dan penerima harus memiliki *stego-key* yang sama dan dirahasiakan dari pihak yang tidak diizinkan untuk mengetahui isi pesan tersebut. Penerima harus menggunakan gambar yang berisi *stego-image* untuk dapat menerima pesan rahasia tersebut.

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.

Dalam penelitian ini, diajukan sebuah algoritma steganografi menggunakan 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 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.

2. 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)
g. Algoritma B217AN

2.1 Steganografi

Steganografi diterapkan di berbagai bidang dan aplikasi seperti badan intelijen [Rebecca T. Mercuri. 2005], badan militer [P. Wayner], citra medis [R Rodriguez-Colin, F.-U. Claudia, and G. de J. Trinidad-Bias. 2007], [Y. Li, C. T. Li, and C. H. Wei. 2007], penyiaran TV [N.F. Johnson, S. Jajodia. 1998], *Checksum embedding* W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb. 2000], struktur data tingkat lanjut [H. Pang, K. L. Tan, and X. Zhou. 2003], [S. Hand and T. Roscoe. 2002], Sistem radar dan penginderaan jarak jauh.

Teknik Transform Domain, menyembunyikan informasi dalam bit dari *cover images* sehingga sangat sesuai dengan teknik seperti kompresi dan *cropping*. Teknik *Transform Domain* yang paling umum adalah transformasi kosinus diskrit dan transformasi *wavelet*, perbandingan antara jumlah informasi rahasia yang harus disematkan dengan kesulitan membaca pesan rahasia [B. Li, J. He, J. Huang, and Y.Q. Shi. 2011]. Spread spectrum mencakup gambar sebagai *noise* atau menambahkan noise ke *cover images*.

Selanjutnya adalah teknik statistik yang juga disebut sebagai teknik yang memodifikasi karakteristik dari *cover images* dan mencegah dari kesalahan dalam proses *embedding*. [S.C. Katzenbeisser. 2000] Modifikasi ini dapat dirasakan oleh manusia dengan mengidentifikasi variasi pencahayaan. Teknik ini rentan terhadap serangan *rotating, cropping, scaling* dan juga semua serangan *watermarking*.

Gambar 2.1 Cover-data. ***Gambar 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].

2.2 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]. Gleick [J. Gleick. 1997] bahwa tidak ada ahli sistem *chaos* yang diwawancarainya setuju dengan definisi dari kata *chaos* itu sendiri.

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].

2.3 Spread Spectrum

Metode *spread spectrum* dalam steganografi diilhami dari 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].

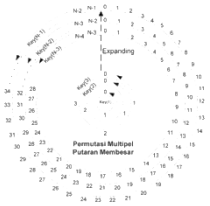
Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan metode *spread spectrum* memperlakukan *cover-object* sebagai derau (*noise*) ataupun sebagai usaha untuk menambahkan derau semu (*pseudo-noise*) ke dalam *cover-object*. *Cover-object* sebagai derau Sistem yang memperlakukan *cover-object* 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*.

2.4 Analisis Stegano

Analisis 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 tersebut diukur kinerjanya terhadap ketahanan gangguan, seperti: perubahan kecerahan dan kontras kompresi JPEG, *Gaussian noise, Poisson noise, Salt and Pepper noise,* dan *speckle noise*, *data loss*.

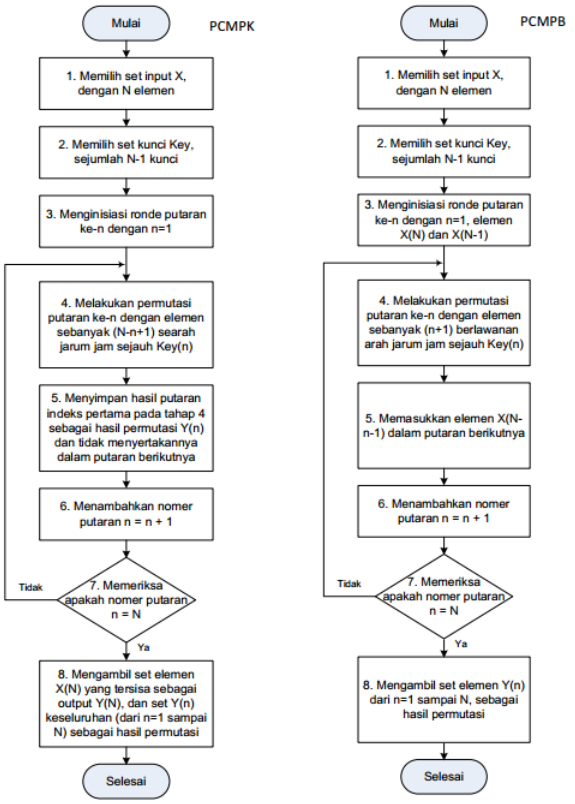
2.5Algoritma Permutasi Chaotic Multiputaran Membesar (PCMB)

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:



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]

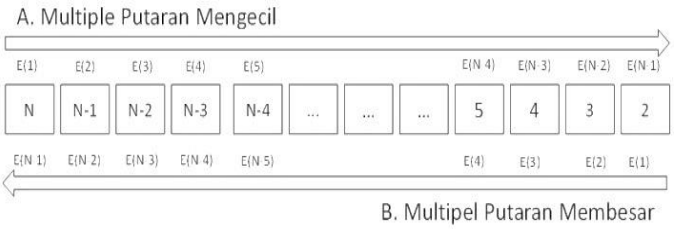
1. Memilih *set* input *X*, dengan *N* elemen.
2. Memilih set kunci *Key* sejumlah $N - 1$ rangkaian kunci *Key*(*n*). (*Key*(*n*) dapat dipilih sembarang angka bilangan bulat dalam ruang kunci sesuai dengan Gambar 3.3.
3. Menginisiasi ronde putaran ke-*n* dengan $n = 1$, dua elemen terakhir *X*(*n*) 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.

2.6Algoritma Permutasi Chaotic Multiputaran Mengecil (PCMK)

Metode PCMK ada dua metode yaitu permutasi PCMPK dan PCMPB yang merupakan 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 (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 *setY*(*n*) dari $n = 1$ sampai *N* sebagai hasil permutasi PCMPK.

2.7 Algoritma B217AN

Algoritma B217AN merupakan algoritma steganografi baru, yang dibuat berbasis PCMPK/B menggunakan metode *spread spectrum*. Proses dilakukan pada penyisipan pesan terbagi menjadi yaitu PCMK, *spread image*, transformasi frekuensi, domain frekuensi, modulasi,

retransformasi dan *stego image* (pesan rahasia disisipkan kedalam gambar).

Proses yang dilakukan pada ekstrasi pesan terbagi menjadi yaitu retransformasi image, domain frekuensi, demodulasi, *spread image*, PCMB, proses akhir menghasilkan kunci dan *information image*.

3. METODOLOGI PENELITIAN

3.1 Perancangan Algoritma B217AN

Tahapan perancangan Algoritma B217 yaitu:

1. Pada pengirim pesan, yaitu melakukan pemilihan media *cover-image* yang akan digunakan dan memasukkan pesan rahasia (*embedded-image*) yang akan disisipkan.
2. *Embedding process* untuk dimasukkan ke *cover-image* menggunakan *spread spectrum.* Menghasilkan keluaran yaitu *stego-image* yang telah dimasukkan *embedded-image* dan citra telah tersisipi yang akan terlihat.
3. Tahap ketiga yaitu citra stego diuji kehandalannya dengan beberapa serangan, proses tersebut menghasilkan keluaran yaitu citra stego yang diserang.
4. Tahap keempat menghasilkan keluaran yaitu citra stego yang telah diserang. Pada penerima, *stego image* diekstraksi untuk menghasilkan pesan rahasia yang tersimpan di dalam *cover image*.

Blok diagram steganografi pada citra digital adalah sebagai berikut:

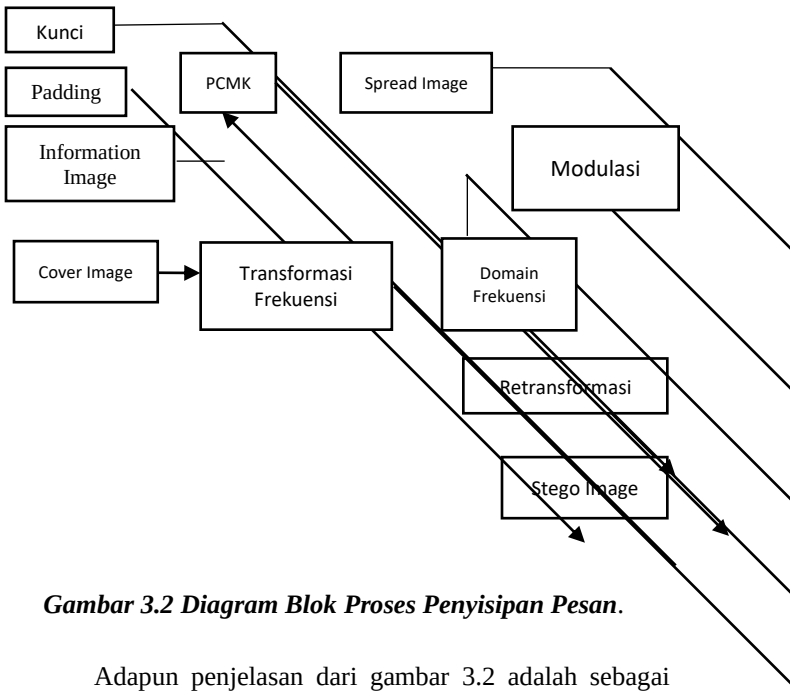
Gambar 3.1 Diagram Alir Sistem.

Adapun penjelasan dari gambar 3.1 adalah sebagai berikut:

1. Tahap pertama yang dilakukan adalah pada pengirim pesan, yaitu melakukan pemilihan media *cover-image* yang akan digunakan dan memasukkan pesan rahasia (*embedded-image*) yang akan disisipkan.
2. Tahap kedua yaitu *embedding process* untuk disisipkan ke dalam *cover-image* dengan menggunakan metode *spread spectrum*. Proses tersebut menghasilkan keluaran yaitu *stego-image* yang telah disisipkan pesan rahasia (*embedded-image*) dan citra yang telah tersisipi yang akan terlihat.
3. Tahap ketiga yaitu citra stego diuji kehandalannya dengan beberapa serangan, proses tersebut menghasilkan keluaran yaitu citra stego yang telah diserang.
4. Tahap keempat menghasilkan keluaran yaitu citra stego yang telah diserang. Pada penerima, *stego image* diekstraksi untuk menghasilkan pesan rahasia yang tersimpan di dalam *cover image*.

3.2 Proses Penyisipan Pesan

Diagram Blok proses penyisipan pesan pada citra digital adalah sebagai berikut:



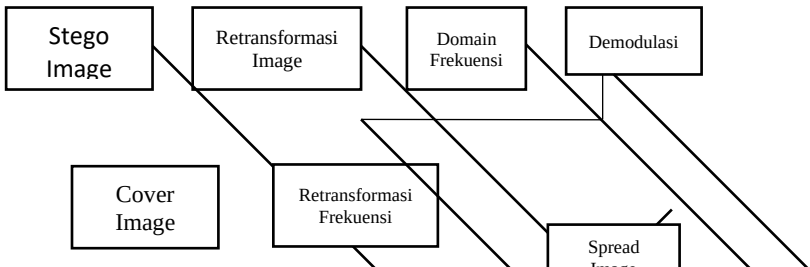
Gambar 3.2 Diagram Blok Proses Penyisipan Pesan.

Adapun penjelasan dari gambar 3.2 adalah sebagai berikut:

1. Mempersiapkan kunci yang akan digunakan, kunci tersebut akan digabungkan dengan *padding* dan *information image* kemudian diproses dengan metode PCMK (Permutasi *Chaotic* Multiputaran Mengecil).
2. Setelah melalui proses PCMK, akan menghasikan *spread image*. Hasil dari *spread image* masuk ke modulasi.
3. Pada tahapan *cover image*, langkah yang dilakukan adalah transformasi frekuensi dan hasilnya akan masuk ke modulasi.
4. Setelah melalui tahapan modulasi, kemudian dilakukan retransformasi sehingga menghasilkan *stego image* yang sudah disisipi kunci dan *information image*.

3.3 Proses Ekstrasi Pesan

Diagram Blok proses ekstrasi pesan pada citra digital adalah sebagai berikut:



Gambar 3.3 Diagram Blok Proses Ekstrasi Pesan.

Adapun penjelasan dari gambar 3.3 adalah sebagai berikut:

1. Tahap awal dari proses ekstrasi pesan yaitu dari *stego image* yang telah dihasilkan dari proses penyisipan pesan, kemudian dilakukan *retransformasi image*.
2. Setelah dilakukan *retransformasi image*, tahapan selanjutnya adalah mengubah menjadi domain frekuensi.
3. Pada tahap selanjutnya adalah demodulasi dari proses domain frekuensi.
4. Setelah melalui proses demodulasi, maka akan menghasilkan *spread image*. *Spread image* tersebut diproses menggunakan PCMB (Permutasi *Chaotic* Multiputaran Membesar), dari proses PCMB akan menghasilkan kunci, *information image* dan *padding*. Pada hasil akhir, *padding* tidak digunakan.

4. PEMBAHASAN

Algoritma steganografi B217AN yang dihasilkan merupakan algoritma steganografi yang tahan terhadap gangguan, gangguan yang dimaksud meliputi ketahanan gangguan, seperti: perubahan kecerahan dan kontras kompresi JPEG, *Gaussian noise*, *Poisson noise*, *Salt and Pepper noise*, dan *speckle noise*, *data loss*.

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

4.1 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;
%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);
```

4.2 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
```

5. KESIMPULAN

Algoritma steganografi digabungkan dengan metode *spread spectrum* berfungsi untuk menyebar informasi yang

terdapat didalam *embedded image* sehingga tidak diketahui keberadaan atau posisi dari pesan yang disisipkan tersimpan, sehingga pengirim pesan pun tidak mengetahui posisi dari pesan yang terdapat didalam *embedded image*.

Kinerja algoritma steganografi yang dihasilkan dapat tahan perubahan kecerahan dan kontras kompresi JPEG, *Gaussian noise, Poisson noise, Salt and Pepper noise,* dan *speckle noise*, *data loss*.

Pada penyisipan pesan menggunakan Permutasi *Chaotic* Multiputaran Mengecil (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 pada hasil akhir dari proses steganografi citra.

DAFTAR PUSTAKA

[1] C. Cachin (2005) : *Digital Steganography*

[2] Cheddad, A. (2007) : "*Strengthening Steganography in Digital Image"s*, Disertasi Program Doktor, University of Ulster, Magee.

[3] D. R. L. Davidchack. (2002, 10/17/2015). "*Bifurcation Diagram"*. Available: http://www.math.le.ac.uk/people/rld8/ma1251/lab3.html.

[4] E. Rasul, Faridnia. Saed, S. Hossein, "*Using the Chaotic map in image steganography"*. International Conference on Signal Processing Systems, 2009.

[5] Ersin Esen, A. Aydın Alatan*, "Comparison of Forbidden Zone Data Hiding and Quantization Index Modulation", Digital Signal Processing* 22 (2012) 181–189.

[6] Hideki Noda, Michiharu Niimi, Eiji Kawaguchi*, "High-performance JPEG steganography using quantization index modulation in DCT domain",* Pattern Recognition Letters 27 (2006) 455–461.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and. Kalker. "*Digital Watermarking and Steganography (Second Edition)*", Morgan Kaufmann Publishers, 2007, ISBN: 978-0-12- 372585-1.

[8] I. Rosziati, K.S. Teoh, *"Steganography algorithm to hide secret message inside an image"*. Computer Technology and Application 2 (2011) 102-108.

[9] Joshi, S. V., Bokil A. A., Jain, N. A., Koshti, D. (2012) : "*Image Steganography Combination of Spatial and Frequency Domain"*, International Journal of Computer Applications, 53, 25 - 29.

[10] L. Kocarev and S. Lian, "*Chaos-based cryptography": theory, algorithms and applications* vol. 354: Springer, 2011.

[11] M. Tabor, "*Chaos and Integrability in Nonlinear Dynamics": An Introduction*: Wiley-Interscience, 1989.

[12] 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.

[13] Munir, R. (2004) : "*Pengolahan Citra Digital", Informatika*, Bandung.

[14] 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.

[15] R. Mutia S "*Studi dan Pengujian Algoritma Steganografi pada Aplikasi Steghide*", Institut Teknologi Bandung, Indonesia. 2017.

[16] S.C. Katzenbeisser. "*Principles of Steganography.*" in Information Hiding Techniques for Steganography and Digital Watermarking, 2000.

[17] S. Hand and T. Roscoe. Mnemosyne: "*Peer-to-peer steganographic storage"*. In 1st Inti. Workshop on Peer-to-Peer Systems, volume 2 429, March 2002, pages 130-140.

[18] S.R. Widianto. "*Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK". Jurnal Multinetics*". Vol. 3. No. 2. 2017.

[19] S.R. Widianto. "*Desain dan Analisa Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Menggunakan Matlab*". *Jurnal Elektra.*Vol. 3. No. 1. 2018.

[20] S.R. Widianto., Y. Suryanto. "*Desain Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) yang Tahan Terhadap Gangguan.*", Prosiding SEMNASTEK Fakultas Teknik Universitas Muhammadiyah Jakarta, 2018.

[21] S. Wiggins, "*Introduction to applied nonlinear dynamical*

systems and chaos" vol. 2: Springer Science & Business Media, 2003.

[22] Supangkat, Suhono H., Juanda, Kuspriyanto. "*Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital"*. ITB, Bandung. 2000.

[23] V.M. Potdar, S. Han, E. Chang*, "Fingerprinted secret sharing steganography for robustness against image cropping attacks"*, Proceedings of IEEE Third International Conference on Industrial Informatics (TNDIN), Perth, Australia, 10-12 August 2005, pp. 717-724.

[24] V.Y Milad, A. Peyman, B.J. Milad, "*High secure digital image steganography based on 3D Chaotic map"*, IKT2015 7th International Conference on Information and Knowledge Technology.

[25] Xian-ting Zeng, Zhuo Li, Ling-di Ping. "*Reversible data hiding scheme using reference pixel and multi-layer embedding"*, International Journal of Electronics and Communications (AEÜ) 66 (2012) 532– 539.

[26] 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.

[27] Y. Suryanto, R. R. Nasser, and R. F. Sari, "*Performance Comparison of TCP Spoofing and End to End Approach to Enable Partial QoS on IP Based Network*," *International Journal of Computers Communications & Control*, vol. 10, pp. 403-419, 2015.

[28] Y. Zhou, L. Bao, and C. P. Chen, "*A new 1D Chaotic system for image encryption*," *Signal processing*, vol. 97, pp. 172-182, 2014.

[29] Z. Xiaohong, M. Lequan, "*Steganography of multimedia information based on generalized chaos synchronization system"*.in: Proceedings of IEEE International Conference on Communications, Circuits and System, 2006.