e-ISSN: 2549-7952
p-ISSN: 2580-3336

Meningkatkan Keamanan Pesan Menggunakan Enkripsi *Arnold Cat Map* Dan Steganografi *Pixel Value Differencing*

Nizar Haris Masruri[1], Kusrini[2], Andi Sunyoto[3]
[1,2,3]Magister Teknik Informatika, Universitas AMIKOM Yogyakarta Jl. Ring Road Utara, Condong Catur, Depok, Sleman, Yogyakarta 55281
E-mail: *[1]*nizar.masruri@students.amikom.ac.id*, [2]kusrini@amikom.ac.id ,[3]andi@amikom.ac.id

Abstrak *– Pesan tidak hanya berupa text, namun juga berbentuk gambar. Sebuah pesan gambar terkadang merupakan informasi yang sangat rahasia contohnya gambar informasi barang bukti. Untuk itu dibutuhkan teknik untuk melindungi pesan tersebut agar tidak diketahui oleh pihak lain. Pixel Value Differencing (PVD) merupakan salah satu teknik penyisipan pesan ke dalam data digital seperti gambar (citra) dengan kelebihan kapasitas penampung yang besar. PVD menghitung selisih nilai piksel dengan cara membagi piksel-piksel citra menjadi blok-blok yang terdiri dari dua buah piksel yang posisinya berdekatan yang digunakan sebagai tempat penyisipan pesan. Untuk meningkatkan keamanan, maka dilakukan enksripsi pada pesan citra agar konstruksi citra menjadi tidak beraturan sehingga tidak mudah untuk diketahui dan dimanipulasi oleh pihak lain. Paper ini akan menggabungkan steganografi PVD dan metode enskripsi Arnold Cap Map (ACM). Untuk mengetahui kualitas citra yang tersisipi pesan, maka dilakukan evaluasi kualitas citra dengan perhitungan nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Hasil pengujian menunjukkan bahwa citra dengan resolusi 512x512 piksel menghasilkan nilai MSE : 0.36311 dan PSNR (db): 57.3356, sedangkan citra dengan resolusi 256x256 piksel menghasilkan nilai MSE : 11.1786 dan PSNR(db) : 42.4521.*

Kata Kunci *— MSE, PSNR, PVD, RSA, Steganografi*.

1. PENDAHULUAN

Teknologi komunikasi memudahkan pertukaran informasi antar manusia [1]. Komunikasi tersebut berjalan melalui jaringan internet yang membuat perpindahan informasi semakin cepat [2]. Namun, internet memiliki dampak negatif salah satunya yaitu meningkatnya kejahatan terhadap pencurian informasi [3]. Maka daripada itu, pemilik dituntut dapat menjaga data-data atau informasi penting dan rahasia agar tidak mudah diketahui oleh pihak lain sehingga tidak terjadi penyalahgunaan [4]. Terdapat beberapa teknik untuk mengamankan pesan antara lain adalah dengan watermarking, steganografi, kriptografi dan tanda tangan digital [5].

Steganografi adalah sebuah seni untuk menyembunyikan pesan rahasia ke dalam sebuah media sehingga tidak terdeteksi oleh indera manusia [6]. Tujuan dari steganografi adalah memanipulasi sebuah media seperti citra untuk menyembunyikan pesan di dalamnya [1]. Terdapat dua jenis steganografi menurut domainnya, yaitu domain spatial dan domain frekuensi [7]. Domain frekuensi dapat menggunakan transformasi domain seperti transformasi diskrit cosine dan transformasi diskrit wavelet [8]. Teknik ini lebih tahan terhadap manipulasi citra [9]. Least Di dalam seganografi citra berbasis spatial terdapat metode yang memiliki kapasitas paling besar dalam penyisipan pesan yaitu metode Pixel Value Diffferencing (*PVD*) [10]. Cara kerja metode *PVD* ini adalah dengan cara membagi media yang akan disisipi pesan menjadi blok-blok piksel yang bertetangga [11]. Blok-blok dibentuk dari dua buah pixel yang berdekatan atau bertetangga [12]. Bit–bit pesan yang akan disisipkan dihitung dengan besarnya kedua piksel tersebut [13].

Bebasnya perpindahan data di dalam internet dan kecanggihan teknologi tidak menutup kemungkinan pihak lain dapat mencuri citra-cover dan mengekstraksinya untuk mendapatkan pesan dari citra-cover tersebut. Maka perlu dilakukan manipulasi terhadap pesan yang akan disisipkan, salah satunya adalah dengan metode kriptografi. Kriptografi sebuah seni penyandian sebuah pesan dengan mengacak isinya tidak beraturan sehingga pesan tersebut tidak dimengerti oleh orang lain [13] (Lahase dkk, 2015). Pesan tidak hanya berjenis text, namun juga bisa berupa gambar [14]. Sehingga kriptografi dapat juga dapat diterapkan pada gambar. Salah satu metode kriptografi yang digunakan untuk mengenkripsi pesan gambar/citra adalah *Arnold Cat Map (ACM).* ACM digunakan untuk mengacak susunan pixel [15]. Konsep dari algoritma ini adalah memutar citra secara terus menerus sehingga menjadi bentuk yang tidak beraturan [16]. *ACM* sebagai salah satu bentuk dari *discrete chaotic map* yang dilakukan dengan menghitung nilai modulo. Parameter dalam *ACM* digunakan sebagai kunci dalam enkripsi data [17]. Telah banyak dilakukan penelitian-penelitian yang terkait dengan algoritma steganografi *PVD* dan kriptografi *ACM* antara lain, Siambaton mengkombinasikan metode steganografi *PVD* dengan kriptografi *Caesar Cipher* [18], Sinduningrum membuat aplikasi penyisipan pesan dengan metode *PVD* menggunakan android [19], Setyanto melakukan enkripsi pada citra berwarna dengan metode kriptografi *Arnold Cat Map (ACM)*

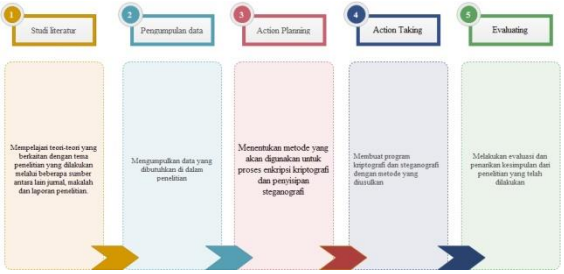
e-ISSN: 2549-7952
p-ISSN: 2580-3336

[15], Purba melakukan enkripsi pada citra dengan dua metode yaitu *ACM* dan *Nonlinear Chaotic Algorithm (NCA)* [20] dan penelitian yang lainnya.

Dengan latar belakang yang telah disebutkan di atas, maka penelitian ini akan melakukan kombinasi teknik steganografi *PVD* untuk penyisipan pesan dan kriptografi *ACM* untuk memanipulasi pesan citra yang akan disisipkan. Kombinasi ini bertujuan untuk memberikan keamanan bertingkat pada pesan citra yang akan dikirimkan.

2. METODE PENELITIAN

Metode penelitian yang dilakukan pada penelitian ini akan ditunjukkan pada Gambar 1 dibawah ini :



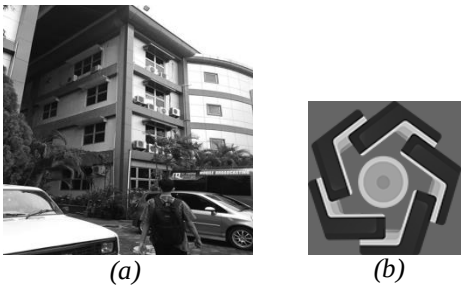
Gambar 1. Alur Penelitian

2.1 Pengumpulan Data

Dalam pengumpulan data, penelitian ini menggunakan metode *generate* (membuat data) yang berupa gambar/citra. Spesifikasi citra yang digunakan antaral lain adalah sebagai berikut :

1. Menggunakan citra grayscale.
2. Citra cover beresolusi 512px x 512px dan 256px x 256px.
3. Citra pesan beresolusi 128px x 128px dan 64px x 64px.

Resolusi citra yang digunakan merupakan resolusi standar yang banyak digunakan untuk penelitian [2]. Citra yang telah digenerate ditunjukkan pada Gambar 2 berikut ini :



(a) *(b)*

Gambar 2. Sampel citra cover yang sudah *(a)* dan pesan citra yang sudah *(b)*

2.2 Action Planning

Action planning adalah tahap perancangan pekerjaan yang akan dilakukan di dalam penelitian ini yaitu dengan menentukan metode yang akan digunakan dan membahas proses yang terjadi di dalam metode.

2.2.1 Arnold Cat Map (ACM)

ACM merupakan pengembangan fungsi chaos ini ditemukan oleh Vladimir Arnold pada tahun 1960, sedangkan kata "*cat*" muncul dikarenakan dia menggunakan citra seekor kucing di dalam eksperimennya [21]. Algoritma *ACM* ini mentransformasikan koordinat pixel (x_i,y_i) pada sebuah citra N ke koordinat baru (x_{i+1},y_{i+1}) yang kemudian membentuk sebuah citra baru N_i. Rumus perhitungan *ACM* ditunjukkan pada Persamaan (1) di bawah ini :

$$\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} Xi \\ Yi \end{bmatrix} mod(N) \dots\dots\dots\dots (1)$$

(x_{i+1},y_{i+1}) adalah posisi pixel yang baru, b dan c adalah kunci rahasia, (x_i,y_i) posisi pixel asli atau posisi semula dan N adalah ukuran *pixel* citra.

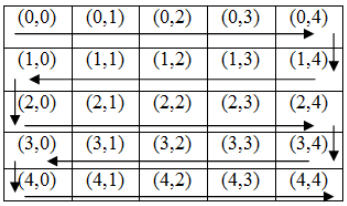
Untuk melakukan deskripsi, maka digunakan Persamaan (2) berikut ini :

$$\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} mod(N) \dots\dots\dots\dots (2)$$

Setelah iterasi terakhir citra hasil sama seperti citra semula. Proses dekripsipun selesai.

2.2.2 Pixel Value Differencing (PVD)

PVD menghitung selisih nilai dua piksel yang bertetangga, dimana hasil selisih kedua piksel tersebut nantinya akan digunakan untuk menyisipkan pesan disembunyikan [11]. Proses urutan perhitungan piksel dimulai dari titik (0,0) yaitu pada piksel paling kiri atas seperti pada Gambar 3 di bawah ini :



Gambar 3. Proses urutan perhitungan antar *pixel* citra pada PVD

Proses penyisipan dilakukan dengan cara membandingkan dua *pixel* yang bertetangga dengan inisialisasi P_i dan P_i+1 [22] dan menggunakan persamaan (3) berikut :

$$d = |P_i - P_{i+1}| \dots\dots\dots\dots\dots\dots (3)$$

Hasil dari perbandingan digunakan untuk mengetahui berapa besar *bit* yang dapat disisipkan ke dalam kedua piksel tersebut. Metode ini menggunakan skema *Wu* dan *Tsai* untuk mengetahui range dari perbandingan piksel sebelumnya. Skema *Wu* dan *Tsai* yang digunakan yaitu :

R={[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]} [22].

Skema ini digunakan untuk mengetahui terdapat di *range* mana selisih dari kedua piksel tersebut, jika telah diketahui dimana letak *range* nya, maka jumlah *bit* pesan yang disisipkan dapat diketahui dengan persamaan (4).

e-ISSN: 2549-7952
p-ISSN: 2580-3336

$t = | Log_2 W_i |$……. (4)

W_i adalah nilai selisih perbandingan dua piksel yang merupakan range dari *d*. Penyisipan dilakukan dengan mengambil sebanyak *t-bit* pesan yang akan disisipkan. Selanjutnya dihitung nilai *difference value* yang baru untuk penyisipan kedalam citra menggunakan persamaan (5) [23].

$d_i = l_i + b$ ……(5)

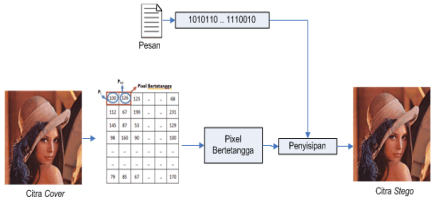
d_i adalah nilai terkecil dari skema *Wu* dan *Tsai*, letak range selisih perbandingan dua piksel yang baru. l_i adalah batas bawah range dua piksel lokasi penyisipan pesan. *b* adalah konversi biner dari *bit* pesan. Untuk menyisipkan pesan ada beberapa aturan yang harus dipenuhi yaitu :

a. Jika $P_i \geq P_{i+1}$ dan $d'_i > d_i$, maka$(P_i+|m/2|, P_{i+1}-|m/2|)$
b. Jika $P_i < P_{i+1}$ dan $d'_i > d_i$, maka$(P_i-|m/2|, P_{i+1}+|m/2|)$
c. Jika $P_i \geq P_{i+1}$ dan $d'_i \leq d_i$, maka$(P_i-|m/2|, P_{i+1}+|m/2|)$
d. Jika $P_i < P_{i+1}$ dan $d'_i \leq d_i$, maka$(P_i+|m/2|, P_{i+1}-|m/2|)$

Dimana *m* didapat dari selisih d_i dengan di dengan menggunakan persamaan (6) di bawah ini :

$m = | d_i - d |$…….. (6)

Proses-proses tersebut dilakukan terus hingga *bit* pesan tersisipi semuanya kedalam citra [10]. Alur dari proses penyisipan pesan ke dalam citra digambarkan sepert pada Gambar 4 di bawah ini :



Gambar 4. Proses penyisipan pesan ke dalam Citra Metode PVD [23]

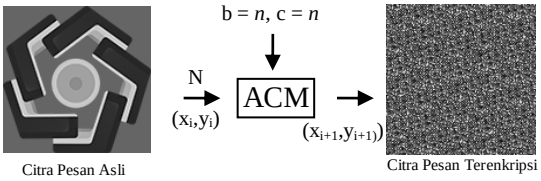
Proses ekstraksi pada metode *PVD* ini adalah mencari selisih P_i dan P_{i+1} untuk mengetahui *d*. Kemudian mengidentifikasi posisi *d* pada skema Wu dan Tsai *R* untuk mengambil nilai l_i dan u_i. Setelah mengetahui keduanya, kemudian mencari nilai $W_i = u_i - l_i + 1$ dan $t_i = {}^2log(W_i)$ untuk mengetahui jumlah bit pesan yang disisipkan. Kemudian menghitung $d_i = d - l_i$, kemudian konversi d_i ke biner dengan panjang t_i. Hasil konversi d_i dengan panjang biner t_i adalah pesan yang disembunyikan.

2.3 Action Taking

Action taking merupakan proses implementasi dari metode yang telah diusulkan pada tahap *2.2* dengan data-data yang telah disiapkan pada tahap *2.1*.

2.3.1 Proses Enkripsi

Proses enkripsi ditunjukkan pada Gambar 5 dibawah ini :



Gambar 5. Proses enkripsi citra

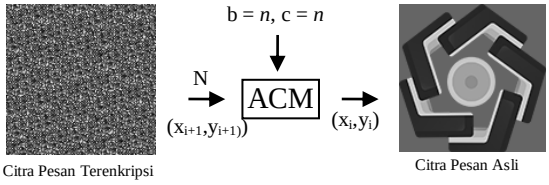
Mengambil (x_i,y_i) dari posisi *pixel* citra asli, mengambil *N* dari ukuran/resolusi citra, kemudian memasukkan nilai rahasia *b* dan *c*. Kemudian di terapkan ke dalam persaman (1). Misalkan mengambil nilai (x_i,y_i) diketahui *pixel (1,1)*, ukuran citra adalah 256x256px, nilai *b* = 1 dan *c* = 1. Maka perhitungannya adalah sebagai berikut :

1. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} Xi \\ Yi \end{bmatrix} mod(N)$
2. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1x1+1 \end{bmatrix} \begin{bmatrix} Xi \\ Yi \end{bmatrix} mod(N)$
3. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1x1+1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} mod(256)$
4. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 1x1+1x1 \\ 1x1+2+1 \end{bmatrix} mod(256)$
5. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} mod(256)$
6. $\begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$

Didapatkan (x_{i+1},y_{i+1}) = (2,3) maka posisi *pixel* (1,1) berpindah ke piksel (2,3).

2.3.2 Proses Deskripsi

Proses deskripsi ditunjukkan pada Gambar 6 dibawah ini :



Gambar 6. Proses deskripsi citra

Mengambil nilai (x,y) misalkan hasil enkripsi yaitu (2,3) dengan ukuran citra 256 x 256 akan dilakukanproses dekripsi dengan kunci *c*=1 dan *b* =1. Maka perhitungannya adalah sebagai berikut :

1. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix}^{-1} \begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} mod(N)$
2. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} \frac{bc+1}{bc+1-bc} & \frac{-b}{bc+1-bc} \\ \frac{-c}{bc+1-bc} & \frac{1}{bc+1-bc} \end{bmatrix} \begin{bmatrix} Xi+1 \\ Yi+1 \end{bmatrix} mod(N)$
3. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} \frac{1+1}{1x1+1-1x1} & \frac{-1}{1x1+1-1x1} \\ \frac{-1}{1x1+1-1x1} & \frac{1}{1x1+1-1x1} \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} mod(256)$
4. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} \frac{2}{1} & \frac{-1}{1} \\ \frac{-1}{1} & \frac{1}{1} \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} mod(256)$
5. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} \frac{2}{1} & \frac{-1}{1} \\ \frac{-1}{1} & \frac{1}{1} \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} mod(256)$

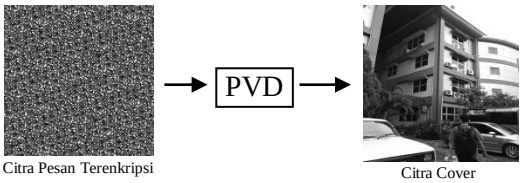
e-ISSN: 2549-7952
p-ISSN: 2580-3336

6. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} 2x2 + (-1)x3 \\ (-1)x2 + 1x3 \end{bmatrix} mod(256)$
7. $\begin{bmatrix} Xi \\ Yi \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Didapatkan (x_i,y_i) = (1,1) maka posisi pixel (2,3) berpindah ke piksel (1,1).

2.3.3 Proses Penyisipan

Penyisipan dilakukan pada pesan yang sudah dienkripsi seperti pada Gambar 7 di bawah ini :



Gambar 7. Penyisipan pesan metode PVD

Langkah-langkah melakukan penyisipan dengan metode *PVD* sebagai berikut :

1. Mengambil pixel citra-cover yang bertetangga yaitu pixel (0,0) dan pixel (0,1). Misalkan nilai kedua pixel adalah 58 dan 120 :

Tabel 1. Contoh potongan pixel citra cover

58	**120**	174
51	203	151
115	104	75

2. Menghitung nilai *differencing value* dari kedua *pixel* tersebut, d = | 58 − 120|, sehingga didapat d = 62.
3. Melihat posisi *continues range* dari d pada skema Wu dan Tsai. R = {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}. Letak *continues range* yang didapat dari d= 62 yaitu [32, 63] dimana l_i = 32, dan J_i = 63.
4. Menghitung kapasitas ruang penyimpanan dari dari kedua *pixel (bit*) yang dibandingkan yaitu t = $LOG^2(63 – 32)$ sehingga didapat = 5 *bit.*
5. Mengambil 5 *bit* dari *pesan citra.*
6. Mengubah nilai *bit* pesan sebanyak t kedalam nilai *decimal*, misalkan 5 *bit* pesan adalah 01010, dirubah menjadi desimal adalah 10 atau b=10, kemudian menghitung nilai *differencing value* yang baru d^i=32+10 => d^i=42.
7. Mencari nilai m sesuai persamaan Wu dan Tsai yaitu $m = |d^i-d|$ => m = |42-62| => m = 20.
8. Melakukan penyisipan pada pixel (0,0) dan (0,1) dengan nilai yang baru sesuai dengan aturan - aturan yang ada, dimana m = 22 Aturan yang terpenuhi yaitu $d^i < d$ dan $P_i < P_{i+1}$ maka P_i =58 + |20/2| dan P_{i+1} = 120 - |20/2| maka didapatkan P_i = 43 dan P_{i+1} = 74 kedalam citra seperti pada Tabel 2 di bawah ini :

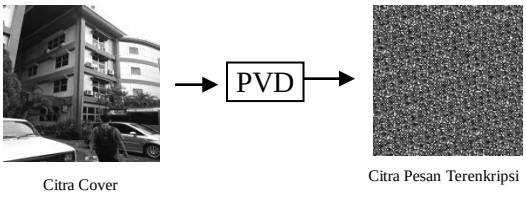
Tabel 2. Contoh potongan pixel citra cover tersisipi

68	**110**	174
51	203	151
115	104	75

Tahapan ini dilakukan sampai semua pesan tersisip ke dalam citra-cover.

2.3.4 Proses Ekstraksi

Proses ini adalah melakukan ekstraksi pesan yang tersisip di dalam citra-cover seperti pada Gambar 8 di bawah ini :



Gambar 8. Ekstraksi pesan metode PVD

Tahapan-tahapan proses ekstraksi pesan PVD antara lain sebagai berikut sebagai berikut :

Tabel 3. Contoh potongan pixel citra cover tersisipi

68	**110**	174
51	203	151
115	104	75

1. Mengambil pixel yang bertetangga yaitu pixel (0,0) dan pixel (0,1) pada Tabel 3.
2. Menghitung nilai *differencing value* dari kedua pixel. d = |110 − 68|, d = 42.
3. Melihat letak *continues range* dari d pada skema wu dan tsai R = {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}. *Continues range* dari d = 42 adalah [32, 63] dimana l_i = 32 dan J_i = 63.
4. Menghitung banyak *bit* dari informasi yang disisipkan di dalam kedua pixel. $T = Log2(63 – 32)$ sehingga didapat t = 5.
5. Merubah nilai decimal ke bentuk *bit* sebanyak t, b = 01010.
6. Proses berikutnya dilakukan berulang sampai semua pixel di ketahui.

2.3.5 Evaluating

Evaluating adalah proses pengujian sebagai parameter keberhasilan serta kekurangan pada penelitian yang dilakukan. Pengujian dilakukan terhadap kualitas citra yang tersisipi pesan. Parameter yang digunakan adalah nilai *Mean Square Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR)* [9]. Adapun standar nilai yang digunakan pada PSNR ditunjukkan pada Tabel 4 di bawah ini :

Table 4. Kualitas citra berdasarkan nilai PSNR [24]

PSNR (dB)	Kualitas Citra
60	Sangat Baik/Tanpa Derau
50	Baik/Derau Sedikit
40	Cukup Baik/Derau seperti butiran
30	Kurang Baik/Banyak Derau
20	Tidak baik/Tidak Layak

e-ISSN: 2549-7952
p-ISSN: 2580-3336

MSE digunakan untuk mengetahui nilai sebuah kesalahan kuadrat rata-rata dengan membandingkan selisih nilai piksel citra awal dan piksel citra hasil dengan ketentuan posisi piksel yang sama. *MSE* dihitung menggunakan persamaan (7).

$$\text{MSE} = \frac{1}{mn} \sum_i^m \sum_j^n || \ I(i,j) - \ K(i,j)||^2 \ldots(7)$$

Penjelasan :
1. MSE = Nilai Mean Square Error
2. (i,j) = koordinat masing-masing pixel
3. n = lebar citra (dalam pixel)
4. m = panjang citra (dalam pixel)

*PSN*R digunakan untuk menyatakan kualitas citra [24]. *PSNR* dengan satuan desibel (*dB*) menunjukkan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal. Untuk menghitung nilai *PSNR* digunakan Persamaan 8 di bawah ini :

$$\text{PSNR} = 10\log\left(\frac{MAX_1^2}{MSE}\right) \ldots\ldots\ldots\ldots\ldots (8)$$

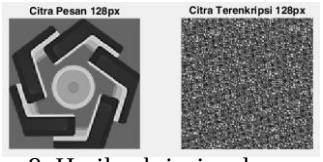
Penjelasan :
1. PSNR = nilai PSNR citra (dB)
2. MSE = Nilai Mean Square Error
3. Max_I = nilai maksimum pixel

3. HASIL DAN PEMBAHASAN

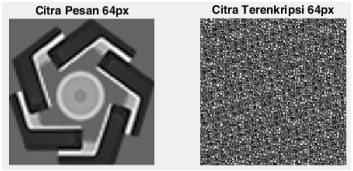
Di dalam penelitian ini digunakan dua buah citra-cover dengan ukuran yang berbeda yaitu 512x512 *pixel* dan 256x256 *pixel*. Serta dua buah pesan-citra dengan ukuran 128x128 *pixel* dan 64x64pixel.

3.1 Proses enkripsi

Keberhasilan enkripsi adalah ketika pesan-citra menjadi citra yang tidak beraturan atau tidak jelas sehingga tidak terdeteksi oleh pihak lain. Hasil dari enkripsi *ACM* pada pesan-citra 128x128px dan 64x64px adalah sebagai berikut :



Gambar 9. Hasil enkripsi pada pesan-citra 128px



Gambar 10. Hasil enkripsi pada pesan-citra 64px

3.2 Kualitas Citra Penyisipan

Kualitas citra penyisipan (*citra-stego*) bisa dikatakan baik jika memiliki nilai PSNR > 50 dB seperti yang telah disebutkan pada Tabel 4. Pengujian dilakukan pada *citra-stego* yang telah disisipi pesan. Hasil nilai *MSE* dan *PSNR* dari masing-masing *citra-stego* ditunjukkan pada Tabel 5 dan Tabel 6 di bawah ini :

Tabel 5. Pengujian nilai *MSE* dan *PSNR* pada citra-stego 512px

Citra-stego 512px		
Citra pesan	MSE	PSNR
128px	1.96368	50.0053
64px	0.36311	57.3356

Tabel 6. Pengujian nilai MSE dan PSNR pada citra-stego 256px

Citra-stego 256px		
Citra pesan	MSE	PSNR
128px	11.1786	42.4521
64px	3.05937	48.0797

4. SIMPULAN

Kesimpulan yang dari penelitian ini antara lain sebagai berikut :

1. Kunci *b* dan *c* pada metode enkripsi *ACM* dapat lebih bervariasi sehingga dapat meningkatkan keamamanan citra.
2. Secara visual, hasil enkripsi ACM menunjukkan citra pesan yang tidak dimengerti.
3. *MSE* dan *PSNR* yang dihasilkan menunjukkan bahwa citra-stego dari metode PVD memiliki kuatas yang baik sesuai dengan Tabel 4.
4. *MSE* dan *PSNR* yang dihasilkan menunjukkan bahwa semakin besar pesan yang dimasukkan, maka semakin menurun kualitas citra-stego yang dihasilkan.

5. SARAN

Saran untuk penelitian selanjutnya antara lain sebagai berikut :

1. Melakukan enkripsi pada citra berwarna.
2. Menggunakan variasi ukuran citra yang lebih banyak.
3. Melakukan pengujian terhadap hasil enkripsi.
4. Membandingkan dengan metode enkripsi citra yang lain.

DAFTAR PUSTAKA

[1] Rachmawanto, E.H. and Sari, C.A., 2017. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System, 2(1), pp.1-11.

[2] Handoyo, A.E., Rachmawanto, E.H., Sari, C.A. and Susanto, A., 2018. Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode

e-ISSN: 2549-7952
p-ISSN: 2580-3336

LSB dan RSA. Jurnal Teknologi dan Sistem Komputer, 6(1).

[3] Susanto, A., Sari, C.A. and Rachmawanto, E.H., 2017, August. Hybrid method using HWT-DCT for image watermarking. In Cyber and IT Service Management (CITSM), 2017 5th International Conference on (pp. 1-5). IEEE.

[4] Wulansari, D., Setyawan, F.A. and Susanto, H., 2016. Mengukur Kecepatan Enkripsi Dan Dekripsi Algoritma RSA Pada Pengembangan Sistem Informasi Text Security. no. Snik, pp.85-91.

[5] Sutojo, T., Rachmawanto, E.H. and Sari, C.A., 2017, August. Fast and efficient image watermarking algorithm using discrete tchebichef transform. In Cyber and IT Service Management (CITSM), 2017 5th International Conference on (pp. 1-5). IEEE.

[6] Anindyawati, N., 2012. Pembangunan aplikasi penyembuyian pesan menggunakan Metode End Of File (EOF) ke dalam citra digital terhadap pesan yang terenkripsi dengan algoritma RSA.

[7] Irawan, C., Sari, C.A. and Rachmawanto, E.H., 2017, November. Hiding and securing message on edge areas of image using LSB steganography and OTP encryption. In Informatics and Computational Sciences (ICICoS), 2017 1st International Conference on (pp. 1-6). IEEE.

[8] Najih, M.N.M., Rachmawanto, E.H., Sari, C.A. and Astuti, S., 2017, November. An improved secure image hiding technique using PN-sequence based on DCT-OTP. In Informatics and Computational Sciences (ICICoS), 2017 1st International Conference on (pp. 47-52). IEEE.

[9] Setyono, A., 2017, October. StegoCrypt method using wavelet transform and one-time pad for secret image delivery. In Information Technology, Computer, and Electrical Engineering (ICITACEE), 2017 4th International Conference on (pp. 203-207). IEEE.

[10] Tseng, H.W. and Leng, H.S., 2013. A steganographic method based on pixel-value differencing and the perfect square number. Journal of Applied Mathematics, 2013.

[11] Wu, D.C. and Tsai, W.H., 2003. A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9-10), pp.1613-1626.

[12] Avinash, K.G. and Joshi, M.S., 2012, November. A Secured Five Pixel Pair Differencing Algorithm for Compressed Image Steganography. In Computer and Communication Technology (ICCCT), 2012 Third International Conference on (pp. 278-282). IEEE.

[14] Lahase, M.S. and Dhole, S.A., 2015. Encryption Method Using Lsb And Rsa Algorithms In Steganography.

[15] Darwis, D., 2015. Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding. EXPERT, 5(1).

[16] Purba, R., Halim, A. and Syahputra, I., 2014. Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm. JSM (Jurnal SIFO Mikroskil), 15(2), pp.61-72.

[17] CAHYA, I.N., 2015. Penyisipan Pesan Pada Gambar Menggunakan Algoritma Arnold Cat Map (Acm), Least Significant Bit (Lsb) Dan Scale Invariant Feature Transform (Sift). Skripsi, Fakultas Ilmu Komputer.

[18] Setiyanto, N.A. and Rachmawanto, E.H., 2018. Pengacakan Citra Digital Berwarna Dengan Kriptografi Arnold Cat Map (Acm). Prosiding SNST Fakultas Teknik, 1(1).

[19] Siambaton, M.Z., 2016. Kombinasi Algoritma Pixel Value Differencing Dengan Algoritma Caesar Cipher Pada Proses Steganografi. CESS (Journal of Computer Engineering, System and Science), 1(2), pp.19-25.

[20] Sinduningrum, E. and Supriyanto, A., 2016. Perancangan Aplikasi Steganografi Berbasis Android dengan Metode Pixel Value Differencing (PVD). MULTINETICS, 2(2), pp.16-23.

[21] Wijaksono, B.A., 2017. Steganografi pada Citra Digital dengan Metode Cat Map dan Outguess. STRING (Satuan Tulisan Riset dan Inovasi Teknologi), 1(3), pp.317-324.

[22] Rahim, R., 2016. Penyisipan Pesan Dengan Algoritma Pixel Value Differencing Dengan Algoritma Caesar Cipher Pada Proses Steganografi. Jurnal TIMES, 5(1), pp.6-11.

[23] Nofriansyah, D. and Rahim, R., 2016. Combination Of Pixel Value Differencing Algorithm With Caesar Algorithm For Steganography. International Journal of Research In Science & Engineering, 2(6), pp.153-159.

[24] Mandal, J.K. and Das, D., 2012. Colour image steganography based on pixel value differencing in spatial domain. International journal of information sciences and techniques, 2(4).