CESS (Journal Of Computer Engineering, System And Science) **p-ISSN :2502-7131**
Vol 1, No 2, Juli 2016 **e-ISSN :2502-714x**

KOMBINASI ALGORITMA PIXEL VALUE DIFFERENCING DENGAN ALGORITMA CAESAR CIPHER PADA PROSES STEGANOGRAFI

Mhd. Zulfansyuri Siambaton
Magister Teknik Informatika
Universitas Sumatera Utara
zoel_fan@live.com

Abstrak*— Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Metode steganografi yang banyak digunakan saat ini masih mempunyai kekurangan dalam hal kualitas, kapasitas, dan ketahanan. Oleh karena itu dibutuhkan metode steganografi lain yang lebih baik lagi, dan untuk menambah keamanan pada informasi, steganografi dapat dikombinasikan dengan kriptografi. Metode steganografi yang digunakan yaitu metode pixel value differencing (PVD). Metode ini dapat menyisipkan pesan lebih banyak pada pixel yang memilik nilai kekontrasan tinggi. Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, digunakan kriptografi. Teknik kriptografi yang digunakan yaitu algoritma caesar cipher. Caesar cipher merupakan algoritma yang digunakan sebagai standar kriptografi. Penelitian yang dilakukan yaitu mengkombinasikan steganografi dengan kriptografi pada citra digital. Kemudian dilakukan pengujian terhadap metode steganografi yang digunakan untuk mengetahui kapasitas citra, performansi dari metode pixel value differencing (PVD), kualitas citra yang dihasilkan, dan ketahanan pesan terhadap manipulasi citra dan steganalysis. Berdasarkan hasil pengujian didapat kesimpulan bahwa dengan menggunakan metode pixel value differencing (PVD), kapasitas citra untuk menyisipkan pesan, lebih kecil dari ukuran citranya, waktu proses pada metode ini cukup cepat, kualitas citra setelah disisipi pesan mempunyai kualitas yang baik, namun metode ini juga masih mempunyai kekurangan, karena tidak tahan terhadap manipulasi dan pada beberapa citra masih terdeteksi oleh aplikasi steganalysis.

***Keywords*— Kriptografi, Steganografi, PVD (Pixel Value Differencing), Caesar Cipher.**

I. PENDAHULUAN

Dokumen Kerahasiaan dan keamanan suatu informasi pada jaman gelobalisasi sekarang ini semakin menjadi kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum dan pribadi. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Ada berbagai cara yang digunakan untuk melindungi data misalnya pemberian password, tetapi cara ini dapat dibobol oleh para pembajak, karena user dapat membuat kemungkinan-kemungkinan kata yang digunakan sebagai password oleh pihak yang menguncinya. Cara lain yaitu dengan Chipertext, dengan cara ini data yang hendak disimpan disandikan terlebih dahulu, akan tetapi cara ini dapat menarik kecurigaan oleh pihak yang tidak bertanggung jawab, sehingga user akan berusaha memecahkan kode-kode penyandiannya, sehingga data tersebut dapat dibajak. Oleh karena itu dibutuhkan suatu cara yang mempu membuat para pembajak tidak curiga dan pemakai tidak langsung mengetahui bahwa ada data yang tersimpan, dan cara itu adalah Steganografi.

Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang banyak digunakan untuk menyembunyikan informasi yaitu citra digital. Penyisipan informasi pada media citra digital dilakukan pada bit-bit pixel yang terdapat pada citra. Penggunaan citra digital sebagai media penampung mempunyai kelebihan karena indera penglihatan manusia memiliki keterbatasan terhadap warna, sehingga dengan keterbatasan tersebut manusia sulit membedakan citra digital yang asli dengan citra digital yang telah disisipkan pesan rahasia.

Metode Pixel Value Differencing (PVD) merupakan salah satu metode yang dapat digunakan dalam pembuatan steganografi. Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain. Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, steganografi dapat dikombinasikan dengan enkripsi,

sehingga informasi yang disisipkan tidak akan mudah dibaca oleh orang yang tidak bertanggung jawab. Salah satu enkripsi yang dapat digunakan yaitu algoritma Caesar Cipher. Metode Caesar cipher berasal dari Julius Caesar, yang merupakan kaisar Roma, ia menggunakan cipher substitusi untuk mengirim pesan ke panglima perangnya. Caesar Chiper dikenal dengan beberapa nama seperti : Shift Cipher, Caesar's Code, atau Caesar Cipher Shif. Metode Enkripsi ini berjenis cipher subtitusi, dimana setiap huruf pada plainteks nya digantikan dengan huruf lain.

II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter seperti bilangan acak dan kunci [1].

Dalam kriptografi klasik, teknik enkripsi yang digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan-bilangan yang sangat besar. Namun, walaupun enkripsi asimetris lebih lama dalam proses komputasi dibandingkan enkripsi simetris, public key cryptography sangat berguna untuk key management dan digital signature[1].

B. Caesar Cipher

Teknik enkripsi substitusi yang pertama kali dikenal dan paling sederhana ditemukan oleh Julius Caesar. Metode yang digunakan dalam Caesar chiper ini adalah dengan mempertukarkan setiap huruf dari plaintext dengan huruf lain dengan interval 3 huruf dari huruf plaintext[2]. Sebagai contoh dapat dilihat berikut ini :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	P	O	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Gbr. 1 Caesar Cipher

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan dialfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut :

teks terang: universitas Prima Indonesia

teks tersandi: xqlyhuvlwdv Sulpd Lqgrqhvld

Proses penyandian (enkripsi) dapat secara matematis menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka, A = 1, B = 2,..., Z = 26. secara matematis dituliskan dengan,

$$C=E(P)=(P+K) \bmod (26)$$

Sedangkan pada proses pemecahan kode (dekripsi), hasil dekripsi adalah:

$$P=D(C)=(C-K) \bmod (26)$$

Setiap huruf yang sama digantikan oleh huruf yang sama disepanjang pesan, sehingga sandi Caesar digolongkan kepada substitusi monoalfabetik, yang berlawanan dengan substitusi polialfabetik.

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan, lalu tuliskan huruf yang sesuai pada sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut.

Alfabet Biasa: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alfabet Sandi: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Teks Asli: MAKAN NASI GORENG

Teks Sandi: PDNDQ QDVL JRUHQJ

Untuk karakter ASCII dari huruf A sampai dengan Z, sebagai berikut:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	77	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Gbr. 2 Karakter ASCII

C. Steganografi

Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan informasi. Steganografi berbeda dengan kriptografi atau metode keamanan informasi lainnya, metode ini yaitu menyembunyikan informasi atau pesan kedalam media lain seperti citra digital, teks, suara atau video sehingga tidak menimbulkan kecurigaan orang lain. Steganografi membutuhkan dua properti, yaitu informasi dan media penampung. Media penampung yang dapan digunakan yaitu citra digital, audio, teks, dan video [1].

Tujuan dari steganografi adalah menyembunyikan data/pesan pada suatu media. Media penampung data/pesan yang akan disembunyikan dapat berupa gambar digital, suara, video dan media lainnya. Jika pada media yang telah disisipi pesan rahasia tersebut terlihat mencurigakan, maka tujuan dari steganografi tersebut tidak tercapai [1].

Teknik steganografi sudah dikenal sejak jaman Yunani dan Romawi kuno.Misalnya dengan mencukur kepala budak, lalu pesan rahasia ditulis pada kulit kepalanya. Setelah rambut budak tersebut tumbuh, budak terebut dikirim untukmenyampaikan pesan rahasia tersebut. Steganografi mempunyai dua proses utama yaitu embed/penyisipan dan ekstrak/pengungkapan. Proses penyisipan merupakan

proses menyisipkan hidden object atau informasi/pesan yang akan disisipkan, ke dalam sebuah cover object atau media penampung, sehingga menghasilkan file baru yang telah tersisipi pesan didalamnya yang disebut dengan stego file. Sedangkan proses ekstrak merupakan proses pengembalian hidden object secara utuh setelah disisipkan ke dalam cover object sehingga pesan dapat dibaca oleh pihak yang berwenang terhadap pesan tersebut [1].

D. Pixel Value Differencing

Pixel Value Differencing (PVD) skema menggunakan nilai perbedaan antara dua piksel berturut-turut diblok untuk menentukan berapa banyak bit rahasia harus tertanam. Ada dua jenis tabel kisaran kuantisasi dalam metode Wu dan Tasi itu. Yang pertama didasarkan pada memilih lebar kisaran [8, 8, 16, 32, 64, 128], untuk menyediakan kapasitas yang besar. Yang kedua didasarkan pada memilih lebar kisaran [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64], untuk memberikan imperceptibility tinggi. Sebagian besar penelitian terkait fokus pada peningkatan kapasitas menggunakan LSB dan proses penyesuaian, sehingga pendekatan mereka terlalu Selaras dengan LSB pendekatan. Ada sangat sedikit penelitian yang berfokus pada desain meja jangkauan. Selain itu, intuitif untuk merancang dengan menggunakan lebar kekuatan dua. Karya ini desain tabel kisaran kuantisasi baru berdasarkan jumlah persegi yang sempurna untuk memutuskan payload dengan nilai perbedaan antara piksel berturut-turut. Penelitian kami memberikan sudut pandang baru bahwa jika kita memilih lebar yang tepat untuk setiap rentang dan menggunakan metode yang diusulkan, kita bisa memperoleh jumlah gambar yang lebih baik dan kapasitas yang lebih tinggi. Selain itu, kami menawarkan analisis teoritis untuk menunjukkan metode kami didefinisikan dengan baik. Hasil penelitian juga menunjukkan skema yang diusulkan memiliki jumlah gambar yang lebih baik dan kapasitas yang lebih tinggi[3].

Proses penyisipan pada metode ini dilakukan dengan cara membandingkan dua pixel yang bertetangga Pi dan Pi+1 dengan menggunakan persamaan (1).

d= |Pi – Pi+1|……(1)

Hasil dari perbandingan tersebut digunakan untuk mengetahui berapa banyak bit yang dapat disisipkan kedalam dua pixel yang dibandingkan. Metode ini menggunakan skema Wu dan Tsai untuk mengetahui range dari perbandingan pixel sebelumnya. Skema Wu dan Tsai yang digunakan yaitu R={[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]} [3].

Skema ini digunakan untuk mengetahui terdapat di range mana selisih dari dua pixel tersebut, jika telah diketahui dimana letak range nya, maka jumlah bit pesan yang disisipkan dapat diketahui dengan persamaan (2).

t = | Log2 wi|……(2)

wi : Nilai terkecil dari skema wu dan tsai, letak range selisih perbandingan dua pixel. Penyisipan pesan dapat dilakukan dengan mengambil sebanyak t bit dari pesan yang akan disisipkan. Selanjutnya dihitung nilai difference value yang baru untuk penyisipan kedalam citra menggunakan persamaan (3) [3].

d'i = li + b ……(3)

di : Nilai terkecil dari skema wu dan tsai, letak range selisih perbandingan dua pixel. Untuk menyisipkan pesan ada beberapa aturan yang harus dipenuhi yaitu :

1. Jika Pi≥Pi+1 dan d' i>di, maka(Pi+|m/2|,Pi+1-|m/2|)
2. Jika Pi<Pi+1 dan d'i>di, maka(Pi-|m/2|,Pi+1+|m/2|)
3. Jika Pi ≥ Pi+1 dan d ' i ≤ di, maka(Pi-|m/2|,Pi+1+|m/2|)
4. Jika Pi<Pi+1 dan d' i≤di, maka(Pi+|m/2|,Pi+1-|m/2|)

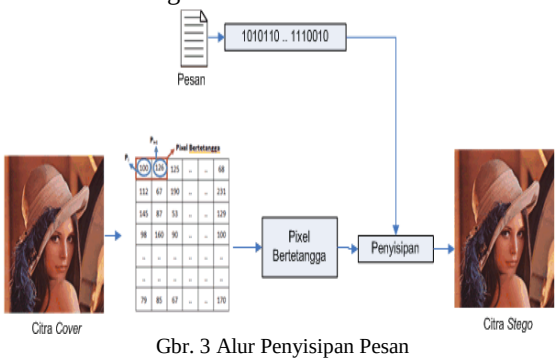
Dimana m didapat dari selisih d'i dengan di dengan menggunakan persamaan

m = | d'i - di|……..(4)

Proses-proses tersebut dilakukan terus hingga bit pesan tersisipi semuanya kedalam citra. Proses ekstraksi pesan dari citra stego menggunakan metode ini dimulai dengan menghitung nilai difference value (di) antara dua pixel yang bertetangga. Nilai difference value tersebut digunakan untuk mengetahui nilai continuous ranges (R) yang sudah didefinisikan menggunakan skema wu dan tsai[3].

1. Analisis Proses Penyisipan

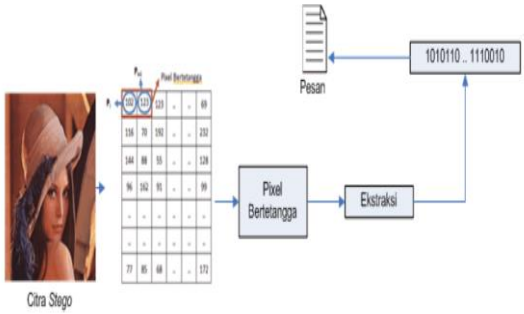
Berikut adalah diagram penjelasan penyisipan pesan yang dilakukan dengan menggunakan metode Pixel Value Differencing.



Gbr. 3 Alur Penyisipan Pesan

2. Analisis Proses Pengungkapan / Ekstraksi.

Proses ekstraksi yaitu proses pengambilan informasi yang tersembunyi pada citra digital. Proses ini akan menghasilkan informasi yang disembunyikan, dengan masukan berupa citra stego-object. Proses ekstraksi pada metode pixel value differencing terlihat pada gambar 4.



Gbr. 4 Proses Ekstraksi Pesan

III. HASIL DAN PEMBAHASAN

Algoritma Caesar merupakan jenis algoritma monoalphabetic yang menukar huruf dari suatu kalimat menjadi huruf lain, pada penelitian ini algoritma Caesar cipher digunakan untuk mengamankan pesan yang akan disisipkan, berikut adalah penerapannya dengan melakukan enkripsi terhadap pesan "UNIVERSITAS PRIMA INDONESIA" dengan jumlah pergeseran sebesar 3 karakter

PESAN = UNIVERSITAS PRIMA INDONESIA
KUNCI = 3

Langkah pertama yang harus dibuat adalah membuat tabel substitusi, seperti dibawah ini :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Gbr. 5 Subtitusi Huruf

Dari tabel diatas dilakukanlah proses enkripsi dengan menerapkan algoritma Caesar cipher, berikut adalah hasil prosesnya:

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (20+3) Mod 26
= (23) Mod 26
=23
=X

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (13+3) Mod 26
= (16) Mod 26
=16
=Q

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (8+3) Mod 26
= (11) Mod 26
=11
=L

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (21+3) Mod 26
= (24) Mod 26
=24
=Y

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (4+3) Mod 26
= (7) Mod 26
=7
=H

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (17+3) Mod 26
= (20) Mod 26
=20
=U

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (18+3) Mod 26
= (21) Mod 26
=21
=V

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (8+3) Mod 26
= (11) Mod 26
=11
=L

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (19+3) Mod 26
= (22) Mod 26
=22
=W

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (0+3) Mod 26
= (3) Mod 26
=3
=D

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (18+3) Mod 26
= (21) Mod 26
=21
=V

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (15+3) Mod 26
= (18) Mod 26
=18
=S

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (17+3) Mod 26
= (20) Mod 26
=20
=U

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (8+3) Mod 26
= (11) Mod 26
=11
=L

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (12+3) Mod 26
= (15) Mod 26
=15
=P

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (0+3) Mod 26
= (3) Mod 26
=3
=D

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (8+3) Mod 26
= (11) Mod 26
=11
=L

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (13+3) Mod 26
= (16) Mod 26
=16
=Q

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (3+3) Mod 26
= (6) Mod 26
=6
=G

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (14+3) Mod 26
= (17) Mod 26
=17
=R

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (13+3) Mod 26
= (16) Mod 26
=16
=Q

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (4+3) Mod 26
= (7) Mod 26
=7
=H

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (18+3) Mod 26
= (21) Mod 26
=21
=V

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (8+3) Mod 26
= (11) Mod 26
=11
=L

Ci = E(P) = (P + K) Mod 26
= (P+3) Mod 26
= (0+3) Mod 26
= (3) Mod 26
=3
=D

Dari hasil proses diatas didapat hasil enkripsi terhadap pesan “UNIVERSITAS PRIMA INDONESIA” dengan pesan “XQLYHUVLWDV SULPD LQGRQHVLD”.

Hasil ciphertext tersebut akan di sisipkan kedalam sebuah file gambar dengan menggunakan algoritma pixel value differencing, Langkah awal yang dilakukan adalah mengubah pesan tersebut menjadi biner seperti dibawah ini

QLYHUVLWDV SRWHQVL XWDPD LV WKH EHVW = 01010001 01001100 01011001 01001000 01010101 01010110 01001100 01010111 01000100 01010110 00100000 01010011 01010010 01010111 01001000 01010001 01010110 01001100 00100000 01011000 01010111 01000100 01010000 01000100 00100000 01001100 01010110 00100000 01010111 01001011 01001000 00100000 01000101 01001000 01010110 01010111

Tahap selanjutnya yaitu mengambil nilai pixel dari suatu citra, diasumsikan suatu citra dengan nama tower.bmp, berikut adalah nilai pixel dari gambar yang

akan disisipkan pesan, nilai pixel didapat dengan menggunakan software matlab.

55 12 167
76 13 175
163 79 202

Setelah mendapat nilai pixel dari gambar, langkah berikutnya adalah melakukan penyisipan pesan, berikut adalah langkah-langkahnya :

1. Mengambil pixel yang bertetangga dari citra yaitu pixel(0,0) dan pixel(0,1), nilai pixel tersebut diambil untuk dilakukan penyisipan, berikut adalah tabel nilai pixel yang bertetangga yaitu 55 dan 112

55	112	167
76	113	175
163	179	202

2. Menghitung nilai *differencing value* dari kedua *pixel* tersebut menggunakan yaitu = | 55 − 112|, sehingga didapat d = 57
3. Mencari letak *continues range* dari nilai *difference value* 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= 57 yaitu [32, 63] dimana ik= 32, dan uk = 63.
4. Menghitung berapa banyak bit dari pesan yang dapat disisipkan kedalam kedua *pixel* yang dibandingkan yaitu $t = \text{LOG}^2(63 - 32)$ sehingga didapat = 5, maka ambil bit dari pesan sebanyak t yaitu 01010.
5. Mengubah nilai bit sebanyak t kedalam nilai *decimal*, dimana 01010 setelah dikonversi menjadi desimal adalah 10 atau b=10, kemudian menghitung nilai *differencing value* yang baru d'=32+10 sehingga didapat nilai d'=42
6. Melakukan penyisipan dengan mengubah nilai dari pixel yang dibandingkan dengan nilai pixel yang baru sesuai dengan aturan – aturan yang ada, dimana m = 15 didapat dari = | 57 − 42|. Aturan yang terpenuhi yaitu $d' < d$ dan $P'_i < P'_{i+1}$ maka P_i =55 + |10/2| dan P_{i+1} = 112 - |10/2|
7. Menyimpan nilai pixel yang baru yaitu P_i = 60 dan P_{i+1} = 107 kedalam citra. Tahapan ini dilakukan sampai semua pesan tersisipi, berikut hasilnya

60 107 167
76 113 175
163 179 202

Nilai gambar diatas merupakan hasil penerapan metode *pixel value differencing*. Setelah proses penyisipan atau biasa disebut dengan decoding pesan, berikutnya adalah proses pembacaan pesan atau biasa disebut dengan decoding pesan. Tahap awal pada proses ekstraksi pesan yaitu mengambil nilai *pixel* dari citra yang telah disisipkan pesan. Jika diketahui citra yang digunakan seperti pada gambar dibawah ini

60 107 167
76 113 175
163 179 202

Tahap selanjutnya yaitu melakukan proses ekstraksi menggunakan metode *pixel value differencing* dengan tahapan-tahapan yaitu sebagai berikut:

1. Mengambil pixel yang bertetangga dari citra. Contoh pixel yang bertetangga yaitu pixel(0,0) dengan pixel(0,1) seperti pada gambar diatas. Nilai dari pixel yang bertetangga tersebut diambil untuk dilakukan penyisipan. Jika Pi dan Pi+1 merupakan pixel yang bertetangga, maka P_i = 60 dan P_{i+1} = 107.
2. Menghitung nilai differencing value dari kedua pixel tersebut menggunakan persamaan d = |60 − 107|, sehingga didapat d = 47.
3. Mencari letak continues range dari nilai difference value 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 = 41 yaitu [32, 63] dimana lk =32, dan uk = 63.
4. Menghitung berapa banyak bit dari informasi yang disisipkan kedalam kedua pixel. Banyak bit tersebut dihitung menggunakan persamaan yaitu $t = Log2(63 - 32)$ sehingga didapat t = 5, atau terdapat 4 bit pesan yang disisipkan pada kedua pixel
5. Mengubah nilai decimal pesan kedalam bentuk bit sebanyak t, maka didapat bit pesan b=01010. Proses berikutnya dilakukan berulang sampai semua pixel di ketahui.

IV. KESIMPULAN DAN SARAN

Kesimpulan dan saran dari penelitian ini, kombinasi algoritma *Pixel Value Differencing* dan *Caesar Cipher* dapat berjalan dengan baik serta hasilnya tidak menimbulkan kecurigaan karena pesan disembunyikan pada citra gambar. Sedangkan saran yang dapat diberikan setelah melakukan pembahasan mengenai penelitian ini, kedepannya algoritma yang dikombinasikan seperti RSA ataupun AES serta pada proses penyisipannya dikembangkan juga kombinasi lain seperti LSB ataupun *patchwork.*

REFERENSI

[1] Kromodimoeljo, S. (2010). Teori & Aplikasi Kriptografi. SPK IT Consulting.
[2] Ardianto, 2011, Implementasi Algoritma Kriptografi Caesar Cipher Pada Aplikasi SMS Telepon Seluler Berbasis J2ME, Yogyakarta
[3] J.K Mandal, Journal of Applied Mathematics, Volume 2013 (2013), Article ID 189706.
[4] Abdul Ghofur, Jurnal Informatika Mulawarman, Vol 5 No.2 Juli 2010.