Triple Transposisi dan Spread Spectrum sebagai Metode untuk Pengembangan Algoritme Steganografi

Herdyan Kharisma Putra[1] dan Sunny Arief Sudiro[2]

[1]Jurusan Teknologi Informasi, Fakultas Teknik Elektro, Universitas Gunadarma
[2]STMIK Jakarta STI&K
herdyan_putra@staff.gunadarma.ac.id,sunny@jak-stik.ac.id

Abstrak

Kerahasiaan data merupakan bagian dari keamanan system, steganografi adalahs salah satu teknik dalam menyembunyikan informasi ke dalam sebuah wadah (media) sehingga data yang disembunyikan menjadi rahasia. Salah satu metode steganografi adalah Spread Spectrum, metode ini merupakan suatu teknik pentransmisian dengan menggunakan pseudonoise code yang terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi, dan de-spreading. Aplikasi ini dibangun dengan bahasa pemrograman Java Android menggunakan Eclipse Helios. Kerahasiaan dari sebuah pesan menjadi salah satu sektor yang menjadi perhatian penulis dalam penelitian ini, sehingga dilakukan penelitian mengenai kombinas pengamanan pesan menggunakan metode Kriptografi. Kriptografi merupakan proses pengamanan suatu pesan dengan mengembangkan pola pembangkit acak sehingga pesan sulit bahkan tidak bisa terbaca saat dibuka oleh orang yang tidak memiliki hak akses. Metode yang dikembangkan merupakan gabungan dari metode Vigènere Cipher dan metode Cipher transposisi.

Kata Kunci : steganografi, triple transposisi, spread spectrum, kriptografi, rahasia.

Pendahuluan

Perkembangan teknologi informasi saat ini bisa dikatakan sangat pesat, hal ini terjadi seiring dengan perkembangan media telekomunikasi terutama smartphone yang berkembang sangat pesat. Smartphone tidak hanya sebagai media komunikasi berupa telepon dan sms melainkan harus dapat memenuhi kebutuhan konsumen yang menginginkan gadget serbaguna. Konsumen menginginkan smartphone yang dapat digunakan sebagai media telpon, sms, koneksi internet sebagai media social media, kamera canggih untuk mengabadikan setiap moment penting namun tetap dengan ukuran yang kecil dan bobot yang seringan mungkin. Kebutuhan akan media serbaguna ini yang dimanfaatkan oleh para produsen smartphone untuk berlomba-lomba membuat gadget canggih dengan tampilan sebaik dan semudah mungkin namun tetap mengutamakan kenyamanan dari penggunanya. Bahkan saat ini banyak orang yang justru memberikan informasi-informasi yang bersifat rahasia melalui media sosial seperti whatsapp dan line. Sedangkan banyak sosial media yang masih dipertanyakan tingkat keamanan data komunikasinya, sehingga keamanan dari pesan para penggunanya masih dipertanyakan. Berdasarkan hal tersebut maka dibutuhkan aplikasi tambahan yang dapat menjamin keamanan dari pesan rahasia yang dikirimkan melalui media sosial.[5]

Pengamanan dari sebuah pesan dapat diwujudkan dengan dua teknik pengamanan, yaitu dengan teknik kriptografi (enkripsi isi pesan) dan steganografi (penyembunyian isi pesan). Kriptografi telah dikenal dan dipakai cukup lama sejak kurang lebih tahun 1900 sebelum masehi pada prasasti-prasasti kuburan. Kriptografi sendiri berasal dari kata “Crypto” yanng berarti rahasia dan “graphy” yang berarti tulisan. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari suatu tempat ke tempat lain. Konsep umum kriptografi yaitu enkripsi dan dekripsi. Dimana enkripsi adalah proses mengubah plaintext (informasi) menjadi ciphertext (pesan dalam bentuk rahasia). Sedangkan dekripsi adalah proses mengembalikan ciphertext pada proses enkripsi menjadi plain-

text semula. Salah satu metode kriptografi adalah Triple Transposition Vigènere Cipher, Triple Transposition Vigènere Cipher adalah metode enkripsi dengan cara mengulang teknik Vigènere Cipher yang setiap plainteksnya dilakukan transposisi terlebih dahulu sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya.[1]

Proses yang terjadi pada Triple Transposition Vigènere Cipher terbagi menjadi dua bagian. Metode transposisi dapat disimbolkan dengan T dan metode substitusi menggunakan vigenere yang disimbolkan dengan E serta kunci untuk melakukan vigenere K. Secara matematis metode Triple Transposition Vigènere Cipher ini dapat dituliskan sebagai: Proses enkripsi: C = S3(T3(S2 (T2(S1(T1(P)))))) Cipherteks diperoleh dengan mentransposisikan plainteks, kemudian hasilnya disubstitusi menggunakan kunci pertama, lalu ditransposisikan kembali, lalu disubstitusi dengan menggunakan kunci yang berbeda dari kunci pertama, disebut saja kunci kedua, setelah itu dilakukan transposisi lagi yang kemudian diakhiri dengan proses substitusi menggunakan kunci ketiga. Substitusi disini menggunakan Vigènere Cipher. Pengamanan pesan dapat juga dilakukan dengan teknik steganografi, steganografi adalah seni dan ilmu tentang komunikasi yang tidak terlihat. Kata Steganografi berasal dari kata Yunani "stegos" yang berarti "penutup" dan "grafia" yang berarti "menulis" sehingga dapat diartikan sebagai "tulisan yang tersembunyi". Tujuan dari Steganografi adalah untuk menyembunyikan data dari pihak ketiga. Biasanya pesan akan dimunculkan dalam bentuk lain: gambar, artikel, daftar belanja, atau beberapa bentuk lainnya[6].

Metode yang dapat digunakan dalam teknik steganografi, salah satunya adalah Spread Spectrum. Metode Spread Spectrum mentransmisikan sebuah sinyal pita informasi sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi. Penyebaran frekuensi sendiri berfungsi untuk menambah tingkat redudansi. Tujuan dari menambah tingkat redudansi adalah agar kode tidak mudah dipecahkan. Proses penyisipan dari metode Spread Spectrum dimulai dari proses penyebaran biner pesan dimulai dari membaca pixel pesan gambar, kemudian rangkaian pixel diubah menjadi array biner, array biner dari pesan akan disebar dengan cara dikalikan dengan faktor pengali untuk penyebaran biner. Proses kedua adalah proses pembangkitan bilangan kunci acak, menggunakan algoritme LCG (Linear Congruential Generator) yang dimulai dari pengubahan kata kunci yang dimasukkan berupa string menjadi biner, kemudian masing-masing rangkaian biner dari kata kunci dilakukan menggunakan fungsi XOR (exclusive OR). Hasil dari proses XOR (exclusive OR) pada kata kunci adalah nilai kata kunci yang akan digunakan sebagai bilangan bulat yang akan dikalikan dengan faktor pengali dalam algoritme LCG. Proses ketiga dari metode spread spectrum adalah penggabungan biner pesan dengan biner kunci acak dengan menggunakan fungsi XOR (exclusive OR). Proses terakhir adalah penyisipan bit-bit kedalam rangkaian bit gambar penampung yang sebelumnya merupakan pixel. Berdasarkan kebutuhan akan keamanan data berupa pesan rahasia ini maka muncul ide untuk melakukan sebuah penelitian mengenai penggabungan kedua teknik pengamanan pesan tersebut menjadi satu metode. Berdasarkan ide penelitian tersebut maka penulis melakukan penelitian penggabungan algoritme Triple Transposition Vigènere Cipher dengan algoritme Spread Spectrum untuk menciptakan metode baru tanpa mengurangi tingkat keberhasilan penyembunyian pesan yang menggunakan algoritme spread spectrum. Hasil dari penelitian ini diharapkan dapat tercipta sebuah metode baru yang dapat memberikan rasa aman terhadap setiap pengguna smartphone dalam bertukar informasi rahasia.[2]

Teknik Kriptografi

Steganografi

Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan di dalam pesan lain sehingga keberadaan pesan yang pertama tidak diketahui. Steganografi berasal dari bahasa Yunani steganos yang berarti tulisan tersembunyi. Steganografi sangat kontras dengan kriptografi. Kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, sedangkan steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi. Dalam prak-

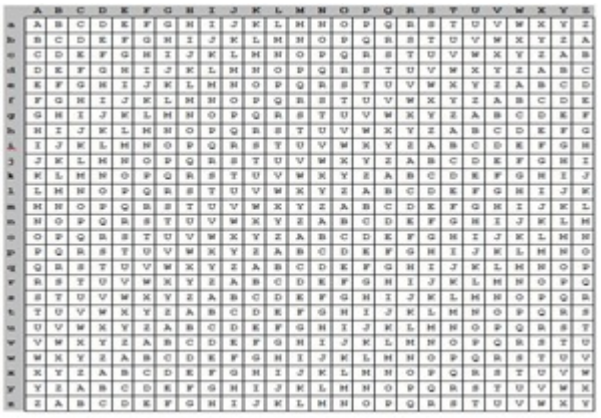
teknya, pesan dienkripsi terlebih dahulu, kemudian disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaan pesan.. Steganografi membutuhkan dua property utama yaitu wadah penampung dan informasi rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Informasi rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video [9][10].

Spread Spectrum

Metode ini adalah penulisan ini, yaitu sebuah teknik pentransmisian dengan menggunakan pseudonoise code, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwidth) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika pseudonoise code tersinkronisasi. Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan Metode Spread Spectrum memperlakukan cover-object baik sebagai derau (noise) ataupun sebagai usaha untuk menambahkan derau semu (pseudonoise) ke dalam cover-object. Proses penyisipan pesan menggunakan Metode Spread Spectrum ini terdiri dari tiga proses, yaitu spreading, modulasi, dan penyisipan pesan ke citra JPEG. Sedangkan Proses ekstraksi pesan menggunakan Metode Spread Spectrum ini terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi, dan de-spreading[3][7].

Algoritme Vigènere Cipher

Pada dasarnya, Vigènere Cipher menggunakan bujursangkar Vigènere Cipher untuk melakukan enkripsi. Setiap baris pada dibujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher. Bedanya, pada Vigènere Cipher, setiap huruf pada plainteks dienkripsi menggunakan kunci yang berbeda. Huruf pertama pada plainteks dienkripsi dengan kunci yang berupa huruf pertama pada kata kunci dan begitu seterusnya. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Gambar 1 memperlihatkann table Bujursangkar Vigènere Cipher[4][8].



Gambar 1: Tabel Bujursangkar Vigènere Cipher

Algoritme Cipher Transposisi Cipher transposisi adalah mengubah susunan huruf pada plainteks sehingga urutannya berubah. Plainteks yang dirubah susunan hurufnya seperti ini merupakan cipherteksnya. Nama lain untuk metode ini adalah permutasi, karena transpose setiap huruf didalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Plainteks: AYAH PERGI KE KANTOR

Metode Zigzag 3 baris

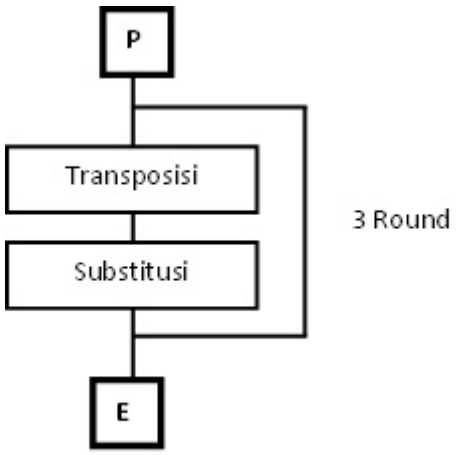
A			P			I			A			R		
	Y	H		E	G		K	K		N	O			

Cipherteks: APIARYHGKKNOARET

Metodologi Penelitian

Triple Transposition Vigènere Cipher

Triple Transposition Vigènere Cipher (TTVC) adalah metode enkripsi dengan cara mengulang teknik Vigènere Cipher yang setiap plainteksnya dilakukan transposisi terlebih dahulu lalu dilakukan subtitusi dengan menggunakan tabel bujursangkar, proses ini berulang sebanyak tiga kali dengan menggunakan kunci yang tiap kuncinya harus berbeda satu dengan yang lainnya. Metode Triple Transposition Vigènere Cipher dapat digambarkan pada gambar 2.



Gambar 2: Tahapan proses TTVC

Semua proses enkripsi maupun dekripsi tidak terlepas dari tabel Bujursangkar Viegenere, untuk mempermudah dalam pembuatan logic dari tabel maka penulis membuat formulasi dari tabel Bujursangkar Viegenere.

Metode Penggabungan Setelah mempelajari Algoritme Triple Transposition Vigènere Cipher maka didapat formula pengembangan nya sebagai berikut:

Proses enkripsi:
C = S3(T3(S2(T2(S1 (T1(P))))))
Proses dekripsi:
P = T1'(S1'(T2'(S2' (T3'(S3'(C))))))

Formula tersebut merupakan alur utama proses enkripsi menggunakan Algoritme Triple Transposition Vigènere Cipher, cara membaca formula tersebut adalah P merupakan Plaintext, T merupakan Transposisi, dan S merupakan Subtitusi. Semua langkah tersebut akan dilakukan secara berulang sebanyak 3 kali demi mendapatkan hasil enkripsi yang lebih menjamin tingkat keamanannya.

Hasil dan Pembahasan

Pembuktian Metode Penggabungan

Setelah mempelajari Algoritme Triple Transposition Vigènere Cipher maka didapat formula pengembangan nya dan disajikan pada gambar 3.

Proses enkripsi:
C = S3(T3(S2(T2(S1 (T1(P))))))
Proses dekripsi:
P = T1'(S1'(T2'(S2' (T3'(S3'(C))))))

Sebagai pembuktian maka dilakukan percobaan secara manual, dan dijabarkan sebagai berikut:

Cipherteks :
Y Y X T R I A U B Y T A X V F G I W P Y D L U F J B C J V
Plainteks :
I N I A D A L A H P L A I N T E K S K R I P T O G R A F I

Gambar 3: Formula pengembangan TTVC

Cipherteks tersebut yang kemudian di olah dengan metode spread spectrum, dimulai dengan proses merubah cipherteks kedalam bentuk biner sehingga dapat dilakukan manipulasi pixel gambar yang nantinya akan disisipkan nilai biner dari chiperteks pesan yang ingin disembunyikan.

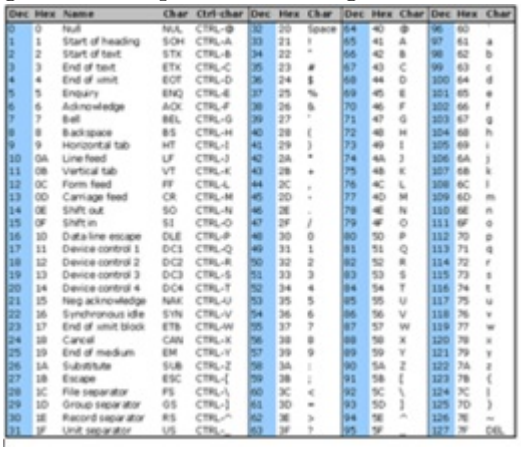
Berikut ini penjelasan dari tiap proses penyisipan cipherteks kedalam gambar menggunakan metode spread spectrum.

Langkah 1: Menyiapkan cipherteks yang akan diubah kedalam bentuk biner. Cipherteks

: Y Y X T R I A U B Y T A X V F G I W P Y D L U F J B C J V

Langkah 2: Mengubah tiap karakter cipherteks kedalam bentuk biner berdasarkan tabel kode ASCII.

Berdasarkan Tabel kode ASCII diatas maka cipherteks akan diubah kedalam bentuk biner, hal ini berlaku untuk keseluruhan cipherteks yang akan disisipkan kedalam gambar.



Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Sebagai contoh diambil 4 karakter pertama dari cipherteks yang dimiliki.

Cipherteks :

Y Y X T R I A U B Y T A X V F G I W P Y D L U F J B C J V

Contoh cipherteks yang digunakan adalah : Y Y X T

Maka berdasarkan tabel kode ASCII karakter huruf Y memiliki nilai 89, karakter X memiliki nilai 88 dan karakter T memiliki nilai 84, nilai karakter tersebut berada dalam bentuk desimal sehingga harus dilakukan konversi bilangan dari desimal kedalam bentuk biner.

Y = 89 = 0 1 0 1 1 0 0 1

Y = 89 = 0 1 0 1 1 0 0 1

X = 88 = 0 1 0 1 1 0 0 0

T = 84 = 0 1 0 1 0 1 0 0

Langkah 3: Setelah didapat nilai biner dari tiap karakter cipherteks maka tiap nilai biner cipherteks tersebut dikalikan 4 sesuai dengan besar faktor pengali yang terdapat pada teori.

Karakter 1 = Y x 4 adalah sebagai berikut:

0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1

Hasil dari pengali diatas dibaca menurun ditiap kolomnya sehingga didapat hasil sebagai berikut :

Yx4 : 0000 1111 0000 1111 1111 0000 0000 1111

Karakter 2 = Y x 4 adalah sebagai berikut:

0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1
0	1	0	1	1	0	0	1

Hasil dari pengali diatas dibaca menurun ditiap kolomnya sehingga didapat hasil sebagai berikut :

Yx4 : 0000 1111 0000 1111 1111 0000 0000 1111

Karakter 3 = X x 4 adalah sebagai berikut:

0	1	0	1	1	0	0	0
0	1	0	1	1	0	0	0
0	1	0	1	1	0	0	0
0	1	0	1	1	0	0	0

Hasil dari pengali diatas dibaca menurun ditiap kolomnya sehingga didapat hasil sebagai berikut :

Xx4 : 0000 1111 0000 1111 1111 0000 0000 0000

Karakter 4 = T x 4 adalah sebagai berikut : T = 84 = 0 1 0 1 0 1 0 0

0	1	0	1	0	1	0	0
0	1	0	1	0	1	0	0
0	1	0	1	0	1	0	0
0	1	0	1	0	1	0	0

Hasil dari pengali diatas dibaca menurun ditiap kolomnya sehingga didapat hasil sebagai berikut :

Xx4 : 0000 1111 0000 1111 0000 1111 0000 0000

Setelah proses perubahan diatas maka akan dihasilkan segmen baru, yaitu :

0000 1111 0000 1111 1111 0000 0000 1111
0000 1111 0000 1111 1111 0000 0000 1111
0000 1111 0000 1111 1111 0000 0000 0000
0000 1111 0000 1111 0000 1111 0000 0000

Langkah 4: Pembangkitan nilai pseudonoise dengan bibit pembangkit yang ditentukan berdasarkan inputan dari User/ Pengguna, saat ini diambil contoh menggunakan kata kunci “sonny”. Nilai pseudonoise didapat dengan cara merubah setiap karakter yang terdapat didalam kata kunci kedalam bentuk biner melalui nilai decimal yang didapat dari tabel kode ASCII sebelumnya. Setelah didapat nilai biner dari tiap karakter maka dilakukan operasi gerbang logika XOR terhadap setiap karakter kata kunci.

Contoh : s = 01110011 dan o= 01101111

Setelah didapat hasil dari proses gerbang logika XOR antara biner karakter s dengan biner dari karakter o maka dilanjutkan hingga biner dari karakter terakhir.

```
s =   01110011
o =   01101111
      00011100
n =   01101110
      01110010
n =   01101110
      00011100
y =   01111001
      01100101 ⟶ 101 (decimal)
```

Proses diatas menunjukkan hasil dari proses gerbang logika XOR terhadap seluruh karakter kunci adalah 01100101, jika dikonversi kedalam bentuk decimal menjadi 101. Nilai 101 inilah yang kemudian akan dijadikan kunci untuk mendapatkan bilangan acak. Perhitungan pembangkitan bilangan acak sesuai dengan rumus pembangkitan bilangan acak LCG adalah sebagai berikut:

Xn+1 = (aXn + c) mod

a = 17 c = 7 m =84 Xn = bilangan bulat ke-n

Perhitungannya adalah sebagai berikut :
X1 = (17 * 101 + 7) mod 84 hasilnya X1 = 44
X2 = (17 * 44 + 7) mod 84 hasilnya X2 = 83
X3 = (17 * 83 + 7) mod 84 hasilnya X3 = 74
X4 = (17 * 74 + 7) mod 84 hasilnya X4 = 5
X5 = (17 * 5 + 7) mod 84 hasilnya X5 = 8
Demikian seterusnya untuk X6, X7, X8...Xn

Sebagai contoh dilakukan lima kali penyebaran dan hasilnya hasilnya adalah “44 83 74 5 8” jika diubah dalam bentuk biner menjadi:

00101100 01010011 01001010 00000101 00001000

Hasil modulasi bisa didapatkan dengan melakukan modulasi segmen pesan dengan pseudonoise signal menggunkan fungsi XOR (Exlusive OR). Segmen pesan :

0000 1111 0000 1111 1111 0000 0000 1111
0000 1111 0000 1111 1111 0000 0000 1111
0000 1111 0000 1111 1111 0000 0000 0000
0000 1111 0000 1111 0000 1111 0000 0000

Pseudonoise signal:
00101100010100110100101000000101000010000

Maka hasil proses modulasi antara segmen pesan dengan pseudonoise signal menggunakan fungsi XOR adalah :

0010 0011 0101 1100 1011 1010 0000 1010
0000 0111 0000 1111 1111 0000 0000 1111
0000 1111 0000 1111 1111 0000 0000 0000
0000 1111 0000 1111 0000 1111 0000 0000

Hasil dari proses modulasi inilah yang akan disisipkan ke bit-bit gambar. Hasil modulasi tersebut diselipkan diantara bit bit gambar dalam ukuran warna per pixel. Sehingga hal ini dapat mengurangi kecurigaan terhadap pesan rahasia yang terdapat didalam sebuah citra gambar.

Pengujian Citra

Dalam pengujian citra digunakan untuk dapat mengetahui kekurangan serta kelebihan yang terdapat pada aplikasi steganografi citra ini. Penulis melakukan pengujian aplikasi steganografi citra terhadap lima buah citra dengan ukuran gambar serta panjang dan lebar pixel yang berbeda-beda. Aplikasi steganografi citra ini menyisipkan pesan ke dalam citra dengan menggunakan kata kunci atau key. Citra asli dan citra hasil proses encode (stego-object) yang digunakan berformat JPEG. Tabel 1 merupakan contoh gambar yang digunakan untuk pengujian aplikasi steganografi citra

Tabel 1: Citra yang diujikan

No.	Nama Citra	Citra Asli	Pixel X Pixel
1	Android.jpg		960 X 800
2	Bokeh.jpeg		596 X 380
3	HelloKitty.jpg		1920 X 1200
4	Owl.jpg		249 X 320
5	Sanrio.jpeg		960 X 768

Pengukuran Tingkat Kesalahan dan Perbandingan Puncak Kebisingan

Pada pengukuran Kesalahan atau disebut Mean Sequare Eror (MSE) merupakan pengukuran jumlah kesalahan antara citra asli dengan citra hasil encode (stego-object). Jika semakin kecil nilai dari MSE yang didapat maka

akan lebih baik. Pada perbandingan kebisingan atau disebut dengan Peak Signal to Noise Ratio (PSNR) merupakan perbandingan antara nilai maksimum yang diukur dengan besarnya kesalahan yang berpengaruh pada sinyal tersebut biasanya diukur dalam satuan decibel (dB). Jika semakin besar nilai dari PSNR yang didapat maka akan lebih baik. Rumus MSE :

$$MSE = \frac{1}{(MN)} \sum_{i=0}^{m} \sum_{j=0}^{n} \| I(i,j) - I^{'}(i,j) \|^2$$

Keterangan :
MSE = Nilai Mean Square Eror citra
M = Panjang citra (pixel)
N = Lebar citra (pixel)
I = Nilai bit dari citra pada koordinat (x,y)
I' = Nilai bit dari stego-object pada koordinat (x,y)

Rumus PSNR :

$$10 \log_{10} \left(\frac{Max_I^2}{MSE} \right) = 20 \log 10 \left(\frac{Max_I}{\sqrt{MSE}} \right) = 20 \log_{10} \left(\frac{255}{\sqrt{MSE}} \right)$$

Dari perhitungan diatas didapatkan hasil dari nilai Mean Square Eror (MSE) dan Peak Signal to Noise Ratio (PSNR) yang dapat dilihat pada tabel 2.

Tabel 2: Hasil Perbandingan

No	Nama Citra	PESAN A		PESAN B	
		MSE	PSNR(dB)	MSE	PSNR(dB)
1.	Android.jpg	0.003528	72.6644	0.0033867	72.833
2.	Bokeh.jpg	0.0003576	82.5968	0.0002825	83.6206
3.	HelloKitty.jpg	0.2132816	54.8413	0.2126736	54.8537
4.	Owl.jpg	0.0055346	79.6999	0.00502	71.1238
5.	Sanrio.jpg	0.003955	72.1593	0.0038099	72.3217

Tabel 2 menunjukkan hasil perbandingan citra gambar yang sama disisipkan 2 pesan yang berbeda (panjang pesan berbeda dan isi pesan berbeda).

Penutup

Aplikasi steganografi citra menggunakan gabungan metode Triple Transposition Vigènere Cipher dan metode spread spectrum telah berhasil dibuat. Pada aplikasi steganografi citra berisi tiga menu utama yaitu menu encode yang digunakan untuk menyisipkan pesan kedalam citra bertipe data jpeg atau jpg. Pada menu decode digunakan untuk mengekstraksi citra yang telah disisipkan pesan sebelumnya sedangkan pada menu about digunakan untuk mendefinisikan aplikasi yang dibuat beserta cara penggunaan aplikasi. Kemudian pada tahap implementasi maka dilakukan pengujian menghitung nilai Mean Square Eror (MSE) dan nilai Peak Signal to Noise Ratio (PSNR) menggunakan lima buah citra yang mempunyai panjang dan lebar piksel yang berbeda. Terdapat dua kali pengujian yang berbeda dengan lima citra yang sama yaitu dengan menyisipkan pesan yang berbeda panjangnya. Pesan pertama panjangnya hanya satu kalimat dan panjang pesan kedua adalah satu paragraf. Proses pengujian dilakukan dengan membandingkan panjang piksel dan lebar piksel serta ukuran dari citra asli dengan citra hasil proses encode atau disebut juga stego-object. Perubahan ukuran citra asli dengan stego-object tidak terlalu berubah banyak ditandai dengan tiga dari lima citra yang terkompresi tidak melebihi setengah dari citra asli. Keamanan pesan yang disisipi pada citra dengan menggunakan metode spread spectrum tergolong aman karena penyebaran bit-bit data yang telah diubah kedalam biner dilakukan secara acak.

Pada aplikasi steganografi citra ini masih banyak kemungkinan pengembangan yang dilakukan guna mencapai penyempurnaan terhadap setiap kekurangan yang dibuat oleh penulis. Kekurangan aplikasi ini diantaranya tidak dapat menyisipkan pesan kedalam media selain citra berformat jpeg diantaranya format bitmap, gif, png, dll dan pada media yang lain seperti pada video, lagu, barcode, dll. Penyempurnaan keamanan dapat dikembangkan kombinasi metode yang lebih baik dengan menggunakan kombinasi algoritme yang lebih baik.

Daftar Pustaka

[1] Agung Wicaksono,dkk, "Analisis transformasi Baik Citra iris Menggunakan Wavelet Haar Berdasarkan Faktor Retensi Koefisien Wavelet", Program Studi Teknik Elektro. Fakultas Teknik. Universitas Diponegoro, 2012.

[2] M.A. Ineke Pakereng, Yos Richard Beeh dan zsonny Endrawan, "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) Antara Waktu Proses dan Ukuran File Gambar", Jurnal Informatika, Vol 6, No 2, DOI: http://dx.doi.org/10.21460/inf.2010.62.90, 2010.

[3] Lisa M. Marvel, "Spread Spectrum Image Steganography", IEEE Transactions on Image Processing, Volume: 8, Issue: 8, Page(s): 1075 - 1083, DOI: 10.1109/83.777088, 1999.

[4] E. O. Morkel, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group, 2005.

[5] Mulyadi, "Membuat aplikasi Untuk Android", Multimedia Center Publishing, Yogyakarta, 2010.

[6] Teddy Nugraha, "Studi dan Implementasi Steganografi Citra Jpeg Menggunakan Metode Spread Spectrum pada Perangkat Mobile Berbasis Android", Program Ganda Teknik Informatika dan Matematika. Universitas Bina Nusantara, 2012.

[7] Adam Putranto, " Steganografi Melalui Media Gambar dengan Metode Spread Spectrum", Program Studi Teknik Informatika Fakultas Teknologi Indormasi, Universitas Kristen Satya Wacana, 2009.

[8] Rinaldi Munir, "Pengolahan Citra Digital dengan Pendekatan Algoritmik. Penerbit Informatika, Bandung, 2004.

[9] Nazrudin H. Safaat, "Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android", Edisi Revisi, Informatika.Bandung, 2012.

[10] Yus Gias Vembrina, "Spread Spectrum Steganografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, 2006.