APLIKASI RANDOMIZE PARITY BIT CODING STEGANOGRAPHY UNTUK MENINGKATKAN KEAMANAN PENYEMBUNYIAN PESAN RAHASIA PADA FILE DIGITAL

I Wayan Candra Winetra, Ni Wayan Wisswani, I Ketut Suja
Politeknik Negeri Bali, Bukit Jimbaran, Badung, Bali, Indonesia
Email : candrawinetra@pnb.ac.id

Abstrak: Steganografi adalah seni penyembunyian pesan rahasia ke dalam sebuah media cover yang telah dimulai sejak jaman Yunani kuno dan masih digunakan dalam perang dunia kedua dimana pesan rahasia ditulis dengan tinta tak terlihat. Di era digital, steganografi berevolusi dimana pesan rahasia disembunyikan di media digital, dengan hampir semua bentuk file digital bisa dijadikan media cover selama bisa dimanipulasi. Berbagai metode telah dikembangkan untuk meningkatkan kemampuan steganografi seperti LSB atau *parity bit coding*. Penelitian ini akan menggunakan metode *parity bit* yang dilakukan secara acak pada byte data yang dikelompokkan dengan MSB. Penyisipan secara acak akan meningkatkan kerahasiaan pesan tersembunyi karena tidak akan terpola, sedangkan pengelompokkan dengan metode MSB akan memberikan keuntungan dimana modifikasi tidak mengubah *file cover* secara signifikan, sehingga sulit dibedakan dari file aslinya..

Kata Kunci: Randomize, Steganography, Parity Bit, MSB

APPLICATION OF RANDOMIZE PARITY BIT CODING STEGANOGRAPHY TO IMPROVE SECRET MESSAGE SECURITY ON DIGITAL FILES

Abstract: *Steganography is the art of concealment a secret message into media cover which has begun since the ancient Greek times, and still used in the second world war where the secret message was written with invisible ink. In this digital era, steganography evolves where the secret message is hidden in digital media, with almost all form of digital files can be used as a cover as long as they can be manipulated. Various methods were developed to enhancing steganographic capabilities such as LSB or parity bit coding. This research will use parity bit method which is done randomly on the byte data that is grouped by MSB. Randomly insertion will increase the confidentiality of hidden message because it will not be patterned, while grouping with MSB method will give an advantage which is the modification doesn't change file cover significantly, so it will be difficult to distinguish from its original file.*

Keywords: *Randomize, Steganography, Parity Bit, MSB*

I. PENDAHULUAN

Menjaga kerahasian pesan dalam sebuah peperangan sangatlah penting, dimana berbagai metode dapat dilakukan dengan tujuan agar pesan tidak jatuh ke tangan musuh. Steganography adalah sebuah teknik penyembunyian pesan pada sebuah media cover yang terinspirasi dari jaman Herodostus di Yunani, dimana pesan disembunyikan dengan cara mentato kepala utusan, kemudian membiarkan rambutnya tumbuh untuk menyembunyikan pesan. Perkembangan selanjutnya yaitu pada perang dunia ke-2, dimana steganography dilakukan dengan menulis pesan menggunakan tinta tidak terlihat.

Pada era digital, steganography dilakukan dengan menyembunyikan pesan rahasia pada file digital sebagai media covernya. Tidak hanya untuk keperluan perang, steganography juga dapat digunakan untuk meningkatkan keamanan pesan atau data pada dunia bisnis, Teknik steganography misalnya dapat digunakan untuk meningkatkan keamanan pembayaran transaksi *online* [8].

Berbagai metode steganography telah dikembangkan, seperti steganography dengan menyembunyikan pesan rahasia dengan metode seleksi *byte* data menggunakan pohon Huffman [6], atau teknik steganography dengan modifikasi *byte* data menggunakan metode Least Significant Bit (LSB) yang dapat diterapkan pada gambar digital [9]. Teknik steganography lainnya pada gambar digital misalnya dengan merubah jarak dari 2 buah channels pixel data dimana range data merepresentasikan data yang disembunyikan dengan data terlebih dahulu dienkripsi dan dikompresi [4]. Selain pada gambar digital, steganography juga dapat diterapkan pada file

audio dengan teknik *enhanced least significant bit modification* [1].

Penelitian lebih lanjut tentang steganography sudah banyak dilakukan, yang menunjukkan metode steganography dapat diterapkan pada hampir semua file digital, selama *byte* data file tersebut dapat dibaca dan dimodifikasi, dimana steganography bukan merupakan cryptography [9]. Berbagai masalah utama dari aplikasi steganography pada file digital diantaranya tingkat keamanan data yang disembunyikan yang dapat diuji dengan melakukan berbagai macam bentuk serangan. Semakin tinggi tingkat kekuatan dan keamanan metode steganography maka semakin kecil kapasitas penyimpanan datanya. Tantangan kedepan dari steganography adalah menemukan metode steganography yang cepat, lebih efektif dan efisien [7].

Untuk menjawab tantangan tersebut, metode yang digunakan dalam penelitian ini adalah kombinasi dari *steganography metode parity bit coding*, dengan pemilihan byte data yang akan disisipkan bit pesan dilakukan secara random, dimana *byte* data yang dipilih secara random tersebut dikelompokkan terlebih dahulu dalam segmen-segmen data yang diseleksi dengan menggunakan metode Most Significant Bit (MSB). Penyisipan bit data pesan rahasia secara random pada kelompok byte data akan mengakibatkan pendeteksian pesan rahasia menjadi sulit karena penyisipan tidak memiliki pola (random), sehingga akan menghasilkan metode steganography yang lebih kuat, tahan terhadap berbagai serangan, namun effektif dan efisien dalam menjaga kualitas dari file media cover.

Metode *parity bit coding steganography* yang menggunakan nilai atau sifat *parity* akan meningkatkan keamanan penyembunyian pesan rahasia disamping juga akan dapat mempertahankan nilai dari signal data media cover [2].

II. METODE PENELITIAN

Penelitian yang dilakukan merupakan jenis penelitian pustaka yang akan didukung oleh penelitian eksperimentasi dengan membangun sebuah program *prototype* untuk mendukungnya. Data digital yang diuji adalah data image bertype BMP, PNG dan data Audio bertype WAVE. Hasil dari pengujian akan dianalisis menggunakan pengujian statistical dengan metode PNSR [3] and MOS [10] untuk menguji kemiripan file digital terstego dengan file asli.

a. Parity Bit Coding dengan Modifikasi LSB (*least significant bit*)

Parity bit coding steganografi pada penelitian ini dilakukan dengan metode penetapan jumlah parity bit genap dan ganjil, dimana jika jumlah nilai 1 dari biner bit cover adalah genap, maka cover diasumsikan menyembunyikan bit 0, sedangkan jika jumlahnya ganjil, maka diasumsikan menyembunyikan bit 1. Untuk modifikasi bit, digunakan metode modifikasi LSB, dengan merubah bit terakhir dari byte cover yang tidak signifikan merubah byte file asli.

Tabel 1. Contoh Penerapan Metode *Parity Bit* Yang Digunakan untuk menyembunyikan karakter A pada cover

Bit Asli	Jum. Nilai '1'	Bit 'A'= 65 = 01000001	Parity Bit (modifikasi bit terakhir)	Jumlah Nilai 1 Hasil
10001010	3	0	10001011	4 (Mewakili 0)
11001101	5	1	11001101	5 (Mewakili 1)
11101101	6	0	11101101	6 (Mewakili 0)
10111011	6	0	10111011	6 (Mewakili 0)
10011101	5	0	10011100	4 (Mewakili 0)
10011111	6	0	10011111	6 (Mewakili 0)
11011001	5	0	11011000	4 (Mewakili 0)
11011011	6	1	11011010	5 (Mewakili 1)

b. Metode Randomize Parity Bit Coding Pada Segmen Data

Metode random yang digunakan dalam penerapan *parity bit* dilakukan pada segmen data dimana segmen ini dikelompokkan berdasarkan nilai MSB *byte* data yang dipilih berdasarkan niai MSB *byte* data sebelumnya secara berkelanjutan. Nilai MSB yang dipakai yaitu 3 bit MSB awal dari masing-masing data:

contoh:

byte data media cover: **101** 11001, maka nilai MSBnya adalah 101 = 5.

Jika nilai MSB dari byte data adalah 0 maka pengelompokan akan dilewatkan ke byte data berikutnya yang nilai MSBnya bukan 0.

Berikut adalah contoh pengelmpokan MSB tersebut:

Tabel 2. Contoh Penerapan Metode Parity Bit yang Digunakan untuk menyembunyikan bit '1010' pada cover

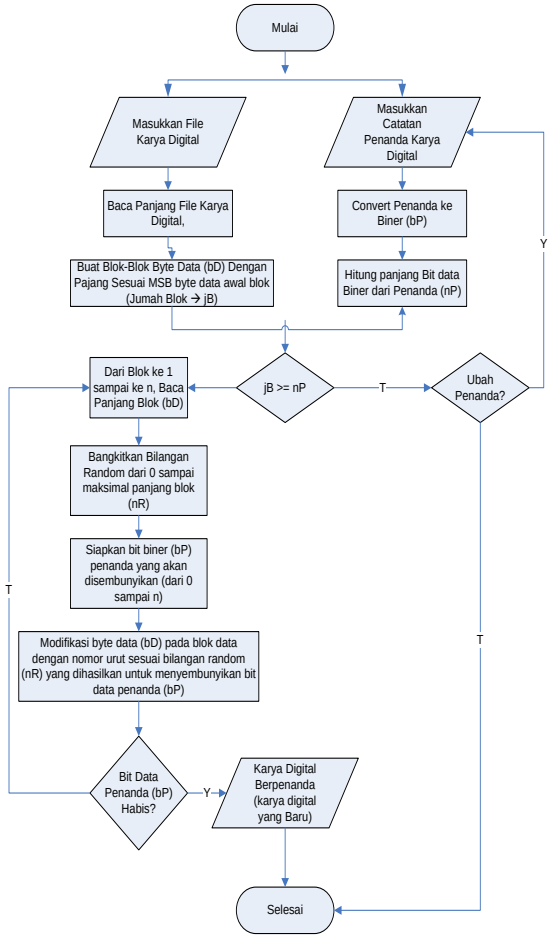
No	Byte Data	MSB	Nilai MSB	PPB	NB	C1	R (PPB)	B = '1010'	BM	C2
1	*10110101*	*101*	*5*	*5*			3			
2	**11100111**	111	7							
3	**01010101**	010	2							
4	**11000110**	110	6		1	22	*	1	11000111	23
5	**00111011**	001	1							
6	**00010011**	000	0							
7	00001101	000	0	0	Skip					
8	*01111010*	*011*	*3*	*3*			2			
9	**01101010**	011	3							
10	**01011001**	010	2		2	15	*	0	**01011000**	14
11	**11011111**	110	6							
12	*00110101*	*001*	*1*	*1*			1			
13	**00001101**	000	0		3	3	*	1	00001101	3
14	00010101	000	0	0	Skip					
15	*10001010*	*100*	*4*	*4*			4			
16	**01111001**	011	3							
17	**01011111**	010	2		4	19		0		20
18	**01010101**	010	2							
19	**11000110**	110	6				*		11000111	
20	00111011	001	1			Dst				

Keterangan:

PPB : Penunjuk panjang blok
NB : Nomor Blok
C1 : Jumlah karakter '1' pada blok
R(PPB) : Nilai random yang dihasilkan dari panjang blok
B(1010) : Bit data yang akan disembunyikan
BM : Byte data hasil modifikasi
C2 : Jumlah karakter '1' pada blok hasil modifikasi

Dari tabel diatas, misalnya byte data pertama yang dibaca adalah '10110101' nilai MSB nya adalah '101', yaitu 5. maka panjang bok data pertama adalah 5 byte berikutnya dari byte file, yaitu: (1) 11100111, (2) 01010101, (3) 11000110, (4) 00111011, (5) 00010011. Dari 5 byte data tersebut akan disembunyikan bit data '1', maka dihitung jumlah '1' dari ke lima byte tersebut, yaitu: 22. karena 22 adalah genap, maka harus dimodifikasi secara parity agar jumlahnya ganjil untuk mewakili bit '1', penentuan byte data yang akan dimodifikasi, dilakukan dengan merandom bilangan 5 (panjang blok), misal nilai random yang didapatkan adalah 3, maka byte data nomor (3) 11000110 yang bit terakhir/LSBnya 0 harus diubah menjadi 1, sehingga hasilnya adalah (3) 11000111, sehingga jumlah karakter '1' pada 1 blok tersebut menjadi 23, yaitu ganjil yang mewakili karakter '1'.

Pengembangan sistem secara umum dapat digambarkan pada Gambar 1.



Gambar 1. Flowchart Sistem

Untuk pembacaan kembali data yang disembunyikan, dapat dilakukan dengan membaca blok data secara MSB, dan menghitung jumlah karakter '1' dari bit data tiap blok tersebut, jika jumlahnya ganjil diasumsikan menyimpan nilai bit '1' dan jika genap maka diasumsikan menyimpan nilai '0'.

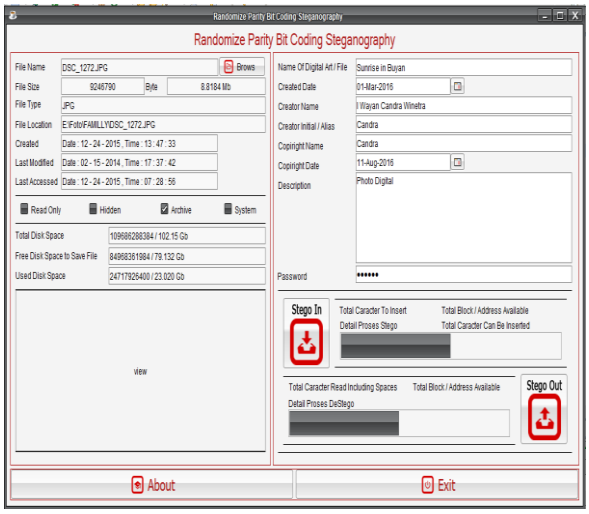
Penyisipan bit data secara random diharapkan dapat meningkatkan keamanan penyembunyian pesan, dimana pola random akan menyulitkan penganalisaan perubahan byte dan meminimalisasi kecurigaan terhadap keberadaan pesan jika dibandingkan dengan penyisipan menggunakan metode terpola.

III. HASIL DAN PEMBAHASAN

Dari percobaan yang dilakukan, berikut adalah hasil yang didapatkan:

a. Antar Muka Aplikasi

penelitian dilakukan dengan membuat sebuah prototype aplikasi untuk membantu eksperimen.



Gambar 2. Sistem yang Dirancang

b. Pengujian Hasil dengan Analisa PNSR

PSNR (Peak Signal to Nois Ratio) menggunakan model matematika standar untuk mengukur perbedaan dua buah signal dimana hasilnya dapat digunakan untuk mengukur tingkat kesamaan atau tingkatan kesalahan signal dengan signal yang lain[5].

$$PSNR = 10 \log_{10} \left(\frac{C^2_{max}}{MSE} \right)$$

Keterangan :

- C^2_{Max} adalah kekuatan sinyal berkas audio setelah proses penyembunyian citra grayscale (nilai signal maximum)
- MSE adalah:

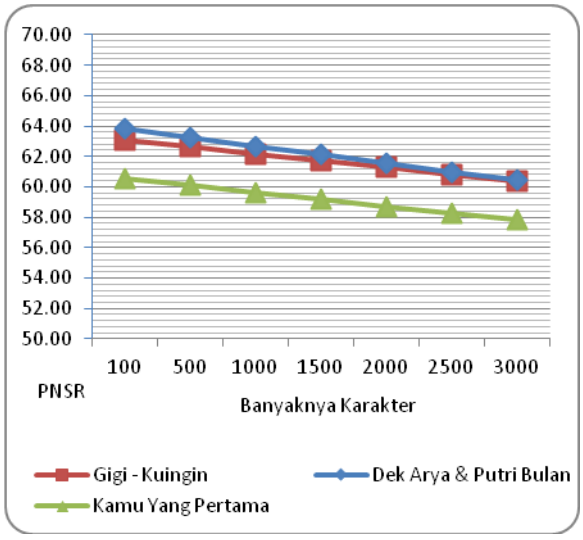
$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} \left(S_{xy} - C_{xy} \right)^2$$

Pada penelitian ini, PNSR digunakan untuk melakukan perbandingan file audio digital sebelum dan sesudah proses steganography.

Tabel 3. hasil dari perhitungan PNSR pengujian:

No	File Wave		Banyaknya Karakter Pesan	Nilai PSNR
	Nama File	Ukuran File (kb)		
1	Gigi - Kuingin	7,869	100	63,085
2		7,869	500	62,632
3		7,869	1000	62,180
4		7,869	1500	61,727
5		7,869	2000	61,274
6		7,869	2500	60,821
7		7,869	3000	60,369
8	Dek Arya & Putri Bulan	3,874	100	63,810
9		3,874	500	63,247
10		3,874	1000	62,684
11		3,874	1500	62,121
12		3,874	2000	61,558
13		3,874	2500	60,995
14		3,874	3000	60,432
15	Kamu Yang Pertama	3,763	100	60,534
16		3,763	500	60,082
17		3,763	1000	59,631
18		3,763	1500	59,179
19		3,763	2000	58,728
10		3,763	2500	58,276
21		3,763	3000	57,825

Grafik Nilai PNSR dari hasil Percobaan



Gambar 3. Grafik nilai PNSR dari hasil percobaan

Dari grafik PNSR yang diuji, menunjukkan bahwa semakin banyak karakter pesan yang disembunyikan maka semakin menurun kualitas dari file hasil steganografi yang ditunjukkan dari menurunnya nilai PNSR yang dihasilkan.

c. Pengujian Hasil dengan Analisa MOS

Pengujian MOS (Mean Opinion Score) dilakukan pada file gambar yang diuji, dengan menyebar kuisioner ke 50 responden yang diminta melakukan perbandingan dan penilaian terhadap gambar sebelum dan sesudah dilakukan steganografi. Rentan nilai yang dipakai yaitu 5 untuk menunjukkan kualitas baik, sampai 1 untuk kualitas yang buruk.

Tabel 4. Rekap dari kuisioner pengujian MOS

No	Jawaban	Gambar						JUM	MOS
		1	2	3	4	5	6		
1	Gambar terlihat sama dan hampir tidak ada perbedaan antara gambar sebelum dan sesudah distegokan pesan	47	46	47	45	45	46	**276**	**5**
2	Gambar terlihat sama tetapi masih terdapat sedikit kesalahan yang terlihat pada gambar yang dihasilkan	3	4	2	4	5	3	**21**	**4**
3	Gambar mirip tetapi terdapat banyak kesalahan yang terlihat pada gambar yang dihasilkan dari proses steganography	0	0	1	1	0	1	**3**	**3**
4	Gambar terdapat banyak bintik dan hasilnya tidak sesuai dengan gambar yang seharusnya	0	0	0	0	0	0	**0**	**2**
5	Gambar berbeda dan terdapat banyak bintik sehingga menggangu gambar semula	0	0	0	0	0	0	**0**	**1**
Jumlah		**50**	**50**	**50**	**50**	**50**	**50**	**300**	

Perhitungan MOS:

$$MOS = \frac{\sum_{i=1}^{n} opinion\_score_i}{n}$$

Dimana n adalah orang yang mengisi kuisioner.
Perhitungan MOS yang dihasilkan:

1. Gambar 1
   MOS = $\frac{47*5}{50}$ = 4.7
2. Gambar 2
   MOS = $\frac{46*5}{50}$ = 4.6
3. Gambar 3
   MOS = $\frac{47*5}{50}$ = 4.7
4. Gambar 4
   MOS = $\frac{45*5}{50}$ = 4.5
5. Gambar 5
   MOS = $\frac{45*5}{50}$ = 4.5
6. Gambar 6
   MOS = $\frac{46*5}{50}$ = 4.6

Rata-rata nilai MOS adalah:

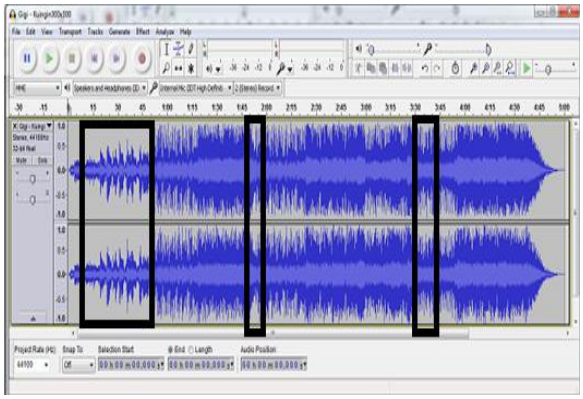
MOS = $\frac{(47 + 46 + 47 + 45 + 45 + 46)}{\text{(max nilai MOS)}} * 5$

$= \frac{276}{300} * 5$

$= 4,6$

d. Pengujian Dengan Perbandingan Histogram

Pengujian ini dilakukan dengan melihat histogram dari file audio wav sebelum dan sesudah dilakukan proses steganography.



Gambar 4. Perbandingan histogram file audio wav "gigi-kuingin.wav"

dari histogram dapat dilihat beberapa bagian dari file audio wav yang berubah setelah dilakukan proses stegangraphy, meskipun demikian perubahan tersbut tida banyak dan tidak signifikan.

IV. SIMPULAN DAN SARAN

Penelitian ini menunjukan bahwa teknik stegangraphy yang diterapkan telah mampu digunakan untuk menyembunyikan penanda hak cipta pada karya digital, dimana dari hasil penelitian dapat disimpulkan bahwa steganografi dengan metode parity bit coding dapat dilakukan secara random pada kelompok byte data yang didapatkan dari nilai MSB, dimana dengan modifikasi byte secara random mampu meningkatkan keamanan penyembunyian pesan dan tidak merubah file asli secara significan yang dapat dilihat dari hasil pengujian PNSR pada nilai rata-rata diatas 50 yang menunjukkan hasil yang baik (mirip dengan file asli, dimana indiator PNSR minimal yaitu 40). Nilai MOS dengan rata-rata 4,6 (pada rentang baik), juga menunjukkan bahwa dengan indera manusia, file hasil steganography sulit dibedakan dengan file asli.

DAFTAR PUSTAKA

[1] Asad, M., Gilani, J. and Khalid A. (2011), An Enhanced Least Significant Bit Modification Technique for Audio Steganography. *In:* Proceedings of IEEE International Conference on Computer Networks and Information Technology, 2011, Bara Gali, 11 July, Pakistan

[2] Burate, D. J. and Dixit, M.R., (2013), Performance Improving LSB Audio Steganography Technique,International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 4, pp. 67-75.

[3] Kaur, J. and Singh, B., (2014), Comparison of LSB and Predictive Coding Using PSNR and MSE, International Journal of Computer Applications, Volume 98, Number 7, pp. 35-38.

[4] Mathkour, H., Al-Sadoon, B. and Touir, A., (2008), A New Image Steganography Technique. *In:* Proceedings of IEEE 4th International Conference on Wireless Communications, Networking, and Mobile Computing, 2008, Dalian, 12 October, China.

[5] M. Kudelka Jr, *Image Quality Assessment* , WDS'12 Proceedings of Contributed Papers, Part I, 94–99, 2012.

[6] Ritchey, P.C. and Rego, V.J., (2012), Hiding Secret Messages In Huffman Trees. *In:* Proceedings of IEEE 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2012, Piraues-Athens, 18 July, Greece.

[7] Roy, R., Changder, S., Sarkar, A. and Debnath, N.C., (2013), Evaluating Image Steganography Techniques: Future Research Challenges. *In:* Proceedings of IEEE International Conference on Computing, Management and Telecommunications (ComManTel), 2013, Ho Chi Minh, 21 January, Vietnam.

[8] Souvik, R. and Venkateswaran, P., (2014), Online Payment System using Steganography and Visual Cryptography. *In:* Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2014, Bhopal, 1 March, India.

[9] Watkins, J. (2001), Steganography - Messages Hidden in Bits, Multimedia Systems Coursework, Department of Electronics and Computer Science, University of Southampton, United Kingdom.

[10] Xu, J., Xing, L., Perkis, A. and Jiang, Y., (2011), On The Properties of Mean Opinion Scores for Quality of Experience Management. *In:* Proceedings of IEEE International Symposium on Multimedia (ISM), 2011, California, 5 December, USA.