

Penyisipan Kode Dalam Sinyal Iklan Radio Siaran Niaga Sebagai Penanda Identitas Kepemilikan

Wahyu Dewanto¹, M. Farid Susanto², Sujoko S.³

Abstract—Advertisements broadcasting service on radio is required to report data after performing broadcast correctly and should be accountable to the owners of ads on the date, hours of broadcasting and the number of ads that aired under the contract. Therefore, it is necessary to monitor the ads in accordance with the contract between the ads owner and the radio broadcaster.

The monitoring can be done by code marking inside the ads as the identity of the owner. The insertion of the Custom DTMF code through the mixing signal was done using the principle of steganography in the time domain.

This research was conducted with a variety of ads audio signal that mixed with noise signal and then analyzed regarding on the placement of the custom DTMF code. For detecting on the receiver side, the DTMF Custom signal must have the magnitude level properly. The results showed that the ads audio signal and the inserted custom DTMF codes can be read well by the detector and it wasn't interfere the ads signal heard by the audience.

Intisari—Layanan siaran iklan di radio membutuhkan adanya laporan yang akuntabel baik mengenai hari, jam, dan berapa kali tayangan dalam sehari yang disepakati dalam kontrak antara pemilik iklan dan radio penyiar. Oleh karena itu sangat penting memonitor hal tersebut dari kedua belah pihak.

Monitoring tersebut dapat dilakukan dengan memberikan tanda di dalam siaran iklannya. Penyisipan kode DTMF Custom melalui pencampuran sinyal ini menggunakan prinsip steganografi dalam kawasan waktu.

Penelitian ini dilakukan dengan berbagai variasi sinyal audio yang dicampur dengan berbagai derau dan dianalisis penempatan kode DTMF Custom-nya. Untuk pendeteksian disisi penerima, sinyal DTMF Custom nya harus mempunyai level yang tepat. Hasil penelitian menunjukkan bahwa sinyal iklan dan kode DTMF Custom yang disisipkan dapat dideteksi dengan baik oleh detector namun tidak terdengar oleh para pendengar.

Kata Kunci— Radioadvertising, code mixing, DTMF custom, and Steganography

I. PENDAHULUAN

Radio siaran (*broadcasting*) merupakan salah satu media yang mampu memberikan atau menyebarkan informasi pada pendengarnya untuk memperoleh berbagai informasi mulai musik, iklan dan berita. Iklan merupakan informasi yang menawarkan produk atau jasa dalam upaya penyampaian pesan atau informasi yang sengaja untuk dipublikasikan seluas luasnya kepada konsumen.

Karena iklan melalui media radio memiliki peranan yang sangat penting dalam bisnis modern, maka antara pemasang iklan dan penyelenggara radio *broadcasting*

perlu melakukan kesepakatan perihal tanggal, jam penyiaran, jumlah iklan yang harus disiarkan dan biaya yang akan dibayarkan. Selain memberikan layanan penyiaran pihak radio *broadcasting* dituntut melaporkan data penyiaran secara benar dan dapat dipertanggung jawabkan kepada pemilik iklan mengenai tanggal, jam penyiaran dan jumlah iklan yang disiarkan sesuai kesepakatan. Tetapi pada pelaksanaan penyiaran iklan, dimungkinkan terjadinya jumlah penyiaran iklan yang tidak sesuai dengan kontrak.

Pemantauan iklan memerlukan suatu mekanisme pengecekan atau pencatatan antara lain : seara manual, pemasang iklan biasanya menyewa seseorang atau lebih yang ditugaskan melakukan pemantauan terhadap siaran yang berlangsung dan mencatat berapa kali iklannya disiarkan. Masalahnya, jam siaran radio *broadcasting* berlangsung dari pagi hingga tengah malam kadang melebihi 18 jam, bahkan ada yang non-stop 24 jam. Jika pemasang iklan mengiklankan lebih dari satu stasiun radio *broadcasting*, maka pemantauan dan pencatatan secara manual tidak efisien dan ekonomis.

Melihat permasalahan ini, diperlukan alat yang mampu mendeteksi jumlah penyiaran iklan yang dapat dipantau oleh pihak pemilik iklannya dan juga penye-lenggara siaran radio. Teknik yang dikembangkan adalah dengan penyisipan kode dalam durasi iklan yang disiarkan. Dengan demikian kedua pihak akan mempunyai record lengkap dan transparan akan jumlah siaran iklannya.

II. TINJAUAN PUSTAKA

Perkembangan teknologi saat ini sangat pesat dalam hal pertukaran informasi yang cepat dan akurat contohnya Internet. Dampak dari banyaknya pengguna dalam melakukan pertukaran informasi salah satunya adalah menyalahgunakan fasilitas tersebut dalam pengiriman dan menyimpan data, agar informasi atau data terjamin kepemilikan dan keasliannya maka perlu dilakukan pengamanan dan cara untuk mengamankan data. Pustaka yang melakukan penelitian atau membahas teknik mengamankan informasi antara lain: Metoda penyisipan *watermark* dengan *spread spectrum modulation* untuk gambar digital dan menggunakan sinyal *pseudo-noise*. Sebagian dari sinyal *pseudo-noise* tersebut dapat dipakai sebagai kunci publik. [1]

Penelitian lain yaitu membandingkan metode *parity coding* dan metode *spread spectrum* pada *audio steganography*. Data yang akan disisipkan berupa teks direpresentasikan dalam bentuk biner, sedangkan data cover menggunakan sinyal audio yang direkam dalam bentuk *wav*. [2]

Selain steganografi, juga diteliti mengenai *watermarking* sebagai suatu teknik menyembunyikan data, aplikasi *watermarking* di berbagai bidang data digital, khususnya aplikasi *watermarking* untuk perlindungan hak cipta serta beberapa metode *watermarking* untuk berbagai jenis data digital, seperti video, gambar, dan audio. [3]

^{1),3} Dosen Jurusan Teknik Elektro dan Teknologi Informasi, Fakultas Teknik Universitas Gadjah Mada. e-mail : wahyud@te.ugm.ac.id, sujoko@mti.ugm.ac.id

²⁾ Mhs S2 Jur. Teknik Elektro dan Teknologi Informasi, Fakultas Teknik Universitas Gadjah Mada. e-mail : mfarids2003@yahoo.com

Selain *steganografi* ada ilmu untuk mendeteksi atau memecahkan informasi tersembunyi yang disisipkan dengan teknik *steganografi* dengan nama *Steganalisis*. [4] Ilmu ini digunakan untuk merusak dan menyerang metode *steganografi*, tetapi juga dapat digunakan untuk mengetes ketangguhan metode *steganografi* yang digunakan. *Steganalisis* menggunakan teknik-teknik dasar dalam manipulasi citra digital dan juga serangan-serangan terhadap *watermark*, seperti *Jitter Attack*, *StirMark*, atau *Mosaic Attack* untuk mendeteksi atau merusak *watermark*. [5]

Watermarking yang digunakan dan mampu melindungi konten *digital audio* dari penyalahgunaan pembajakan *copyright*, ini dibentuk dengan memakai metode *Audio Psychoacoustic Model* dan *Direct Sequence Spread Spectrum (DSSS)*. [6]

Watermarking dengan metode *echo* (gema) digunakan untuk menyembunyikan data dalam file audio. Gema penyembunyian data digunakan untuk menyediakan bukti kepemilikan, penjelasan, dan jaminan integritas konten. Metode ini dapat diterapkan karena kelemahan sistem pendengaran manusia yang memiliki keterbatasan dalam menangkap suara. [7]

A. *Watermarking* dan *Steganografi*

Watermarking adalah metode untuk membubuhkan tanda pada dokumen elektronik yang merupakan aplikasi dari *steganografi* [8]. Namun ada perbedaan antara keduanya; jika pada *steganografi* informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta. Meskipun *steganografi* dan *watermarking* tidak sama, namun secara prinsip proses penyisipan informasi ke dalam data *digital* tidak jauh berbeda.

Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi [9]. *Steganografi* dapat digolongkan sebagai salah satu bagian dari ilmu komunikasi. Kata *steganografi* berasal dari bahasa Yunani: *Stegan*; (tersembunyi) dan *Graptos* (tulisan) yang berarti "tulisan tersembunyi".

Pengertian lain *Steganografi* adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Fungsi dari teknik *Steganografi* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas [10].

Penggunaan *steganografi* antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi, dan melindungi hak cipta suatu produk. *Steganografi* dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan *Steganografi* *ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya.

Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode metode yang dapat digunakan untuk melakukan penyisipan informasi.. Sebagai fungsi yang umum, *steganografi* digunakan untuk

memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi [11]. Untuk tujuan legitimasi dapat digunakan pengamanan seperti citra dengan *watermarking* dengan alasan untuk perlindungan *copyright*. *Digital watermark* (yang juga dikenal dengan *fingerprinting*), sangat mirip dengan *Steganografi* karena menggunakan metode penyembunyian dalam arsip, yang muncul sebagai bagian asli dari arsip tersebut dan tidak mudah dideteksi oleh kebanyakan orang.

Terakhir, *Steganografi* juga dapat digunakan untuk melakukan perawatan atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotase [12], pencurian, atau dari pihak yang tidak berwenang.

Pada penelitian ini yang dilakukan adalah menyisipkan kode ke dalam sinyal audio berisi iklan berformat *wav* dalam kawasan waktu sebagai metode untuk membubuhkan tanda pada dokumen elektronik tersebut. Tujuan teknik penyisipan kode pada sinyal audio berisi iklan dibagian pengirim adalah untuk keperluan penandaan dari kepemilikan iklan agar jumlah tayang iklannya dalam sehari oleh *Radio Broadcasting* dapat dideteksi dan terrekord dibagian penerima.

III. METODE PENELITIAN

A. *Alat dan Bahan*:

Perangkat keras

-Laptop dengan spesifikasi :

- a) *Intel Celeron M350* 1,5 GHz.
- b) 80GB *Enhanced IDE*
- c) 768MB *DDRAM*
- d) 15" *LCD Screen*
- e) *DVD+/-RW/R, CD-RW Combo w/Double Layer Support*
- f) *Genuine Window XP*

-Perangkat penerima radio FM

-Perangkat detektor kode

Perangkat lunak

- a) *Cool Edit Pro 2.1*
- b) *BASCOM (Basic Compiler)*

Tahapan dalam pelaksanaan penelitian ini adalah sebagai berikut :

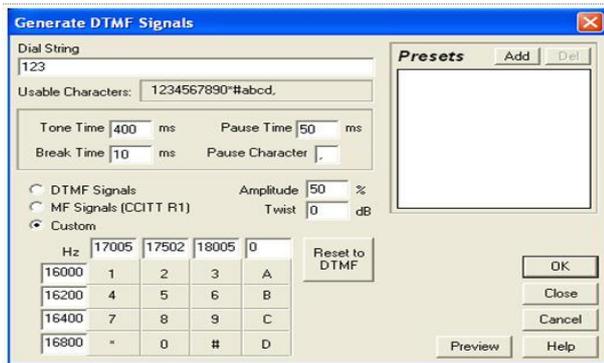
- 1) Merekam audio iklan yang hendak disisipkan kode: dilakukan dengan cara merekam audio iklan dari radio FM atau tempat lain dengan format *wav*, kemudian disimpan di laptop.
- 2) Merancang detektor kode *DTMF Custom*, untuk mengetahui parameter yang dibutuhkan berdasarkan spesifikasi alat yang telah dirancang.
- 3) Membangun program untuk proses encode dan decode
- 4) Mengamati respon penempatan kode dari hasil pencampuran sinyal iklan dari berbagai sisi untuk mendapatkan hasil pembacaan kode yang optimal.
- 5) Mengetes parameter sinyal yang disisipi kode
- 6) Menganalisis data pengukuran dan menyimpulkan.

B. Generator dan Detektor kode DTMF Custom

Pemilihan frekuensi kode DTMF custom didasarkan pada batas kemampuan pendengaran manusia mendengar dari 300 Hz. Sampai dengan 15 kHz. Agar kode tidak terdengar maka daerah frekuensi kode DTMF dibangkitkan pada frekuensi 15998 Hz. sampai dengan 18005 Hz.

Lebar pita (BW) pada radio FM spektrum penuh audio dari 20 sampai 20.000 Hz, tetapi radio FM mem-batasi frekuensi modulasi batas atas sampai 15 kHz. Ini berarti bahwa kode DTMF yang disisipkan berada di atas frekuensi siaran namun masih dalam rentang frekuensi audio. Dengan demikian kode dapat dibaca/dideteksi tetapi tidak terdengar oleh manusia.

Generator sinyal DTMF Custom yang digunakan dalam penelitian ini dibangkitkan dengan software "Cool Edit Pro" v 2,1 seperti ditunjukkan Gbr. 1.



Gbr. 1 Generator DTMF Custom untuk kode "123"

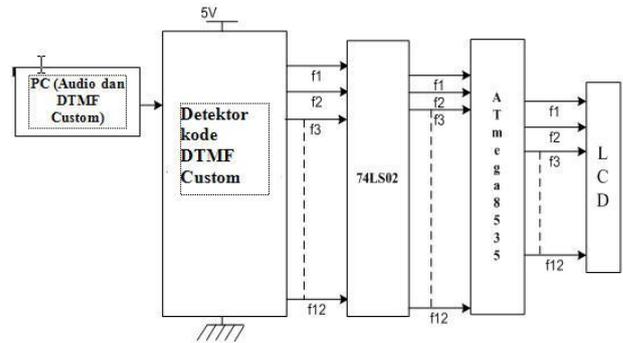
Kode DTMF yang dibangkitkan seperti ditunjukkan dalam Tabel 1 berikut ini. Kode inilah yang diisi pemancar siaran iklan nantinya disisipkan ke dalam sinyal audio iklan.

TABEL I

KODE DTMF CUSTOM YANG DIBANGKITKAN

Low Frequency (Hz)	High Frequency (Hz.)		
	f5 = 17005	f6 = 17502	f7 = 18005
f1 = 15998	1	2	3
f2 = 16205	4	5	6
f3 = 16398	7	8	9
f4 = 16798	*	0	#

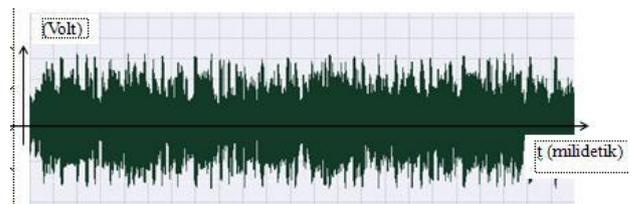
Blok diagram rangkaian detektor kode DTMF Custom dan LCD penampilnya seperti ditunjukkan dalam Gbr. 2. Detektor ini nantinya dipasang disisi penerima/pemantau iklan. Terdapat 12 output dengan nilai-nilai frekuensi yang telah ditentukan.



Gbr. 2 Blok diagram penampil detektor kode DTMF Custom

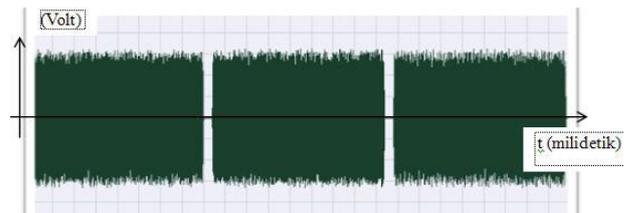
Output ini merupakan kode informasi yang telah disisipkan pada sinyal audio format wav.

Merekam sinyal audio iklan dari siaran radio FM dan menyimpannya dalam laptop yang nantinya "diambil" dalam aplikasi "Cool Edit Pro". Contoh sinyal audio iklan yang direkam seperti pada Gbr. 3.



Gbr. 3 Rekaman sinyal audio iklan format wav

Untuk sinyal kode DTMF Custom yang akan disisipkan dengan kode "123" ditunjukkan dalam Gbr. 4, dan



Gbr. 4 Sinyal kode DTMF Custom "123"

sinyal hasil penyisipan kode DTMF Custom "123" ke dalam sinyal audio iklan ditunjukkan dalam Gambar 5.

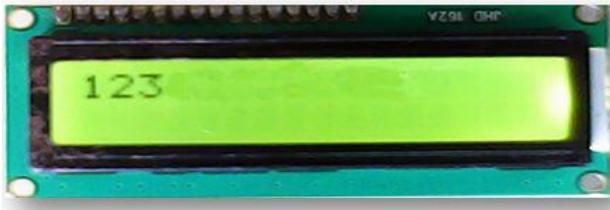


Gbr. 5 Sinyal campuran kode DTMF "123" dan sinyal iklan

Untuk aplikasi penyisipan kode pada audio format WAV dan kode sinyal kode DTMF custom tersebut dapat dilakukan sebagai berikut :

- 1) Buka file audio format WAV.
- 2) Lalu sisipkan kode DTMF Custom pada sinyal audio format WAV dengan metode *Mixing*.
- 3) Pilih "Select File" untuk di mix dengan kode DTMF "123" (sebagai paket kode)
- 4) Hasil *Mixing* seperti pada Gbr. 5

- 5) Sinyal gambar hasil mixing bila di *inputkan* ke dekoder sinyal kodenya ditampilkan oleh LCD seperti pada Gbr. 6

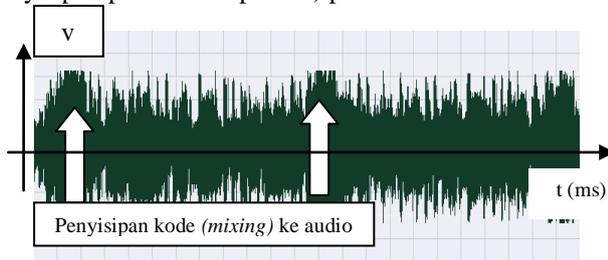


Gbr. 6 Hasil pembacaan dekoder DTMF Custom

Penempatan *mixing* kode DTMF Custom dengan sinyal audio dilakukan dengan 3 pola:

- Pola 1 kode: a. Satu kode diawal audio iklan format *wav*.
 b. Satu kode ditengah audio iklan format *wav*.
 Pola 2 kode: c. Dua kode, satu diawal dan satu ditengah audio iklan format *wav*.
 d. Dua kode, satu diawal dan satu diakhir audio iklan format *wav*.
 Pola 3 kode: e. Tiga kode, satu diawal, satu ditengah dan satu diakhir sinyal format *wav*.

Pola penempatan *mixing* kode poin a sampai e dianalisis keberhasilan terdeteksinya di sisi penerima. Contoh sinyal penyisipan pola 2 kode point c) pada Gbr. 7.

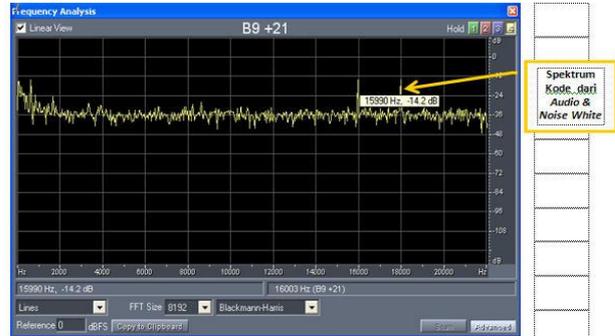


Gbr. 7 Teknik penyisipan 2 kode (*mixing*)

Dalam pemancaran sinyal iklan dari stasiun radio juga diperhitungkan adanya noise akibat kondisi atmosfer, jarak dan *obstacle* antara pemancar dan penerima, yang disimulasikan dengan berbagai tipe noise (*Brown*, *Pink*, dan *White*). Ketiga noise ini dengan *software* "Cool Edit Pro" dapat dilihat spektrum frekuensinya dan level dB magnitudenya.

Sinyal audio iklan kemudian dicampur dengan kode DTMF Custom dan berbagai noise tersebut. Tetapi perlu ditentukan lebih dahulu standar level acuan sinyal audio plus kode DTMF tanpa kontaminasi noise terlebih dahulu. Contoh hasil spektrum frekuensi hasil pencampuran sinyal audio iklan, DTMF Custom dan *White Noise* seperti ditunjukkan dalam Gbr. 8.

Dari Gbr. 8 tersebut, maka dapat diukur nilai SNR (*Signal to Noise Ratio*)nya, dan dapat diperoleh nilai SNR yang dapat terdeteksi oleh detektor DTMF maupun letak penyisipan kode DTMF Custom yang optimum dalam sinyal audio iklan tersebut.



Gbr. 8 Tampilan spektrum campuran sinyal audio Iklan, kode DTMF Custom dan *White Noise*

Agar kode DTMF Custom yang disisipkan dapat terdeteksi dengan baik, maka harus dilakukan percobaan panjang durasi sinyal kodenya. Jika terlalu pendek durasinya, detektor tidak cukup waktu untuk mendeteksinya, namun jika terlalu panjang durasinya akan mengganggu tayangan iklannya. Panjang durasi inilah yang disebut "tone time". Hal lain yang juga sangat penting dicari adalah besarnya *magnitude*/ amplitudo kuat sinyal kode DTMF Customnya. *Magnitude* kuat sinyal kode ini harus memiliki level yang lebih tinggi dari level kuat sinyal iklan ditambah sinyal noise agar dapat dideteksi detektor. Oleh karena itu, perlu dicari batas-ambang nilai SNR (*Signal to Noise Ratio*) antara sinyal kode DTMF terhadap sinyal iklan plus noisenya.

Untuk membedakan antara satu pemasang iklan dengan pemasang lainnya, maka sinyal kode DTMF Custom yang digunakan tersusun atas 3 digit desimal. Perlu dicari waktu jeda antar sinyal digit (disebut "break-time") agar cukup waktu bagi prosesor mengenali masing-masing digit dari sinyal kode DTMF Customnya.

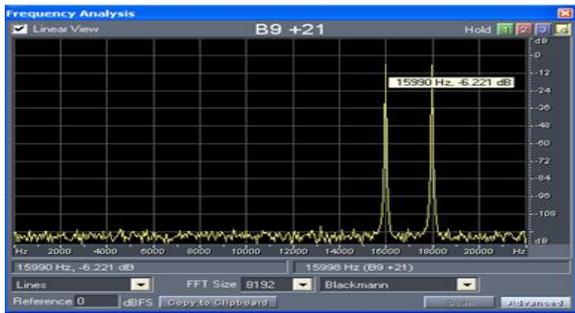
IV. HASIL DAN PEMBAHASAN

Detektor kode DTMF Custom yang dibuat tampak pada Gbr. 9.



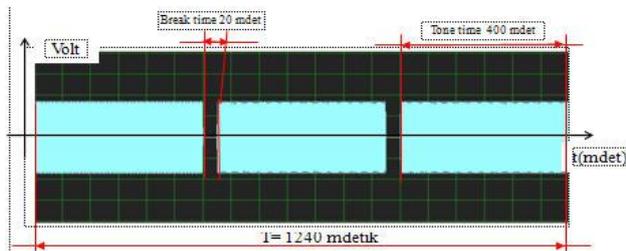
Gbr. 9 Detektor dan Penampil paket kode DTMF Custom

Level amplitudo sinyal kode DTMF Custom yang belum terkontaminasi noise dan digunakan sebagai acuan adalah -6,22 dB (lihat Gbr. 10).



Gbr. 10 Magnitude referensi kode DTMF

Durasi kode DTMF *Custom* (*Tone Time*)nya yang optimum adalah 400 mdetik dengan level minimal -1,866 dB (atau 30% dari level acuan). Penggunaan digit kode DTMF *Custom* yang berbeda (misal "234") atau yang kembar (misal "222") menghasilkan *break time* (lama waktu jeda antar kode DTMF *Custom*) efektif 10 mdetik. Tetapi resiko untuk tidak terbacanya kode kembar tersebut lebih besar dibanding kode yang berbeda, sehingga nilai 20 mdetik cukup aman (lihat Gbr. 11)



Gbr. 11 Tone time dan break time sinyal paket kode DTMF

Dari hasil pengamatan atas berbagai pola penempatan paket kode DTMF *Custom* selama durasi sinyal audio iklan (pola 1 paket-kode, 2 paket-kode, atau 3 paket-kode), baik di awal, di tengah maupun di akhir durasi, detektor DTMF dapat mengenali semuanya. Tetapi penyisipan paket-kode secara serentak di awal, di tengah dan di akhir durasi sinyal audio iklan adalah yang paling efektif untuk menandai kepemilikan iklan tersebut.

Pada level noise -36,35 dB, kode DTMF *Custom* minimal yang terdeteksi berada pada SNR > 9,75 dB. Dalam percobaan diperoleh SNR aman (pasti terdeteksi) adalah 14,3 dB.

V. KESIMPULAN

Dalam penelitian ini telah berhasil dilakukan penyisipan kode DTMF *Custom* 3-digit desimal (paket-kode) dengan menempatkan 3 paket-kodenya di awal, di tengah, dan di akhir durasi sinyal audio iklan. Penyisipan kode ini kedalam sinyal iklan tidak mengganggu informasi iklan yang akan disampaikan ke pendengar, tetapi pendengar dapat memantau jumlah tayangan iklannya.

Paket kode DTMF *Custom* terdiri atas 3 digit dengan jeda antar digit 20 mdetik, durasi masing-masing digit 400 mdetik, dan level kuat sinyal kodenya minimal -1,866 dB, sehingga nilai SNR antara sinyal kode DTMF terhadap sinyal iklan akan terdeteksi dengan baik pada nilai 14,3 dB.

REFERENSI

- [1] Frank H. "Fast Public-Key Watermarking of Compressed Video." Proceedings of the 1997 International Conference of Image Processing (ICIP'97). 1997.
- [2] Riko Arlando Saragih, "Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography". J. T-Elektro Universitas Kristen Maranatha pada Seminar Nasional Aplikasi Teknologi Infor masi 2006 (Snati 2006) ISSN: 1907-5022 Yogyakarta, 17 Juni 2006
- [3] Suhono H. Supangkat, "Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital." Dep.Teknik Elektro, ITB TEKNIK ELEKTRO, Vol. 6, No. 3, 2000
- [4] Edward Ferdian, "Steganalisis Teknik Jitter Attack, StirMark dan Mosaic Attack untuk Merusak dan Menguji Ketangguhan Watermark". Program Studi Teknik Informatika, ITB, 2000
- [5] Rinaldi Munir, "Skema Asymmetric Watermarking berbasis Uji Korelasi" Sekolah Teknik Elektro dan Informatika, ITB, 2007
- [6] Herianto, "Novel Digital Audio Watermarking", Jurusan Teknik Informatika ITB, Bandung, 2000
- [7] Judi Prajetno Sugiono, Yuantoro Setiawan, "Watermarking Pada File Audio PCM Wav Dengan Metode Echo Data Hiding", Sekolah Tinggi Teknik Surabaya Konferensi Nasional Sistem dan Informatika; Bali, 15 Nov 2008
- [8] Thana, Syan "Steganografi pada citra digital dengan Menggunakan Fast Fourier transform. Thesis, 2008, Perpustakaan Pusat UGM, Yogyakarta
- [9] Simmons, G., "The prisoner's problem and the subliminal channel" In *Crypto'83* :hal 51-67, 1983
- [10] Waheed, Q. (2000). "Steganography and Steganalysis" PhD thesis.
- [11] Johnson, N., F., "Exploring Staganography: Seeing the Unseen", IEEE Computer, pp26-34. Feb 1998, <http://isse.gmu.edu/~njohnson/pub/r2026.pdf>
- [12] Bender, W, 1996, "Techniques for data hiding, IBM Systems Journal," Vol 35, No. 3&4, pp 313 -336.